Mathematische Untersuchungen über fehlerkorrigierende arithmetische Codes

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
des
Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von
Armin Ecker
Berlin, Frühjahr 1976

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41547205_0031

Mathematische Untersuchungen über fehlerkorrigierende arithmetische Codes

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
des
Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von
Armin Ecker
Berlin, Frühjahr 1976

1. Referent: Prof.Dr.H.-J.Töpfer

2. Referent: Prof.Dr.B.Eggers

Tag der mündlichen Prüfung:

15.November 1976

UNIV.
LEIDEN
BIBL.

Einleitung

Wie es bereits im Titel zum Ausdruck kommt, ist diese Arbeit allein den mathematischen Aspekten einer Theorie fehlerkorrigierender arithmetischer Codes gewidmet. Mithin schliessen wir alle Implementationsfragen aus. Unter den verschiedenen arithmetischen Codes wiederum beschränken wir uns auf die non-separaten Codes im strengen Sinne, die AN-Codes (Arithmetic Norm). Es bleiben also bis auf einen kurzen Abstecher in Kapitel 1, die non-separaten systematischen Codes und die separaten Multi-Restklassencodes ausgeschlossen. Wie wir im 1. Kapitel zeigen, ist dies mathematisch gesehen keine Einschränkung, da ein enger Zusammenhang zwischen ihnen besteht. Der Unterschied liegt wesentlich in der grundsätzlich verschiedenen Implementation. Einige recht spezielle unter den non-separaten Codes, nämlich solche zur Korrektur von Fehlerbündeln (Burst-Error-Correcting Codes) und diejenigen zur Korrektur Iterativer Fehler (Iterative Errors) werden beiseite gelassen. Ein mit Implementationsfragen eng gekoppelter Problemkreis, der für den praktischen Einsatz von eminenter Bedeutung ist, die Frage nach Decodierungsalgorithmen, wurde nicht bearbeitet.

Sätze und Lemmata der Arbeit sind fortlaufend numeriert, Corollare in Dezimalpunktnotation (z.B. ist Corollar 57.2 das zweite Corollar zu Satz 57). Die Definitionen sind getrennt durchnumeriert. Zahlen in eckigen Klammern verweisen auf das Literaturverzeichnis am Schluss. Sämtliche häufiger oder global erscheinende Bezeichnungen wurden in einer Symboltabelle versammelt (siehe das Inhaltsverzeichnis). Die Bedeutung von Standardnotation ist durch knappe Worte erläutert, eigene Definitionen sind mit der Seitennummer einer Textdefinition versehen. Im Abschnitt 2.3 wird die Theorie der Paare (G, Γ) nach Plotkin [50] vorausgesetzt, zum Verständnis der Abschnitte 4.2 und 4.4 ist eine genaue Kenntnis der Theorie der Totative in dem Umfang wie bei Holzer [30] notwendig (zusätzlich werden die beiden Arbeiten von Müller [45] als bekannt angesehen).

In der Terminologie richten wir uns, was die Theorie der Totative betrifft, streng nach Holzer l.c. und benutzen seine Bezeichnungen ohne jede Erläuterung (ausgenommen wenige Hinweise in der Symboltabelle).

Rechenfehler lassen sich nicht vermeiden, denn irren ist menschlich. So hat man schon von Alters her nach Verfahren gesucht, um solche Fehler zu erkennen. Die einfachste Methode besteht darin, die Rechnung genügend oft zu wiederholen, sei es durch ein- und dieselbe oder verschiedene Personen. Als richtig wird man das Resultat akzeptieren, welches die Mehrzahl aller Rechnungen erbrachte. Eine solche Methode ist teuer, billiger wird es, wenn man nur eine einfachere Kontrollrechnung, eine Probe durchführt. Bei der Addition ganzer Zahlen etwa die Elfer- oder Neunerprobe. Betrachten wir nun (Hardware-) Fehler im arithmetischen Prozessor eines Computers, so können wir über ihre Ursachen genauere Aussagen machen. Es kann z.B. die Steuerungslogik einen Befehl inkorrekt decodieren und einen falschen Algorithmus anstossen oder ein Addierer arbeitet an und für sich falsch. Ein solches Fehlverhalten kann durch Überhitzung, elektrische Felder etc. hervorgerufen werden. Wir fragen wieder nach einem Verfahren, um solche Fehler zu erkennen und/oder zu korrigieren. Es reicht aus, die Integerarithmetik zu betrachten, denn da alle Register endlich sind, können prinzipiell nur ganze Zahlen in einem Rechner dargestellt werden. Da sich alle Operationen auf fortgesetzte Addition zurückführen lassen, genügt es, sich mit Addiemern zu beschäftigen. Ein Weg, um unser Ziel zu erreichen, besteht darin, mehrere arithmetische Prozessoren parallel arbeiten zu lassen und das Ergebnis der Mehrheit als richtig anzuerkennen. Ein Verfahren dieser Art ist unter dem Namen TMR (Triple Modular Redundancy) bekannt: die Ausgänge dreier identischer Blöcke werden über einen majority-vote-taker kombiniert, er lässt das Mehrheitsergebnis passieren. Unter bestimmten Voraussetzungen ist ein solches System sicherer als die einfache Auslegung (vgl. Rao [54]).
Führen wir aus denselben Motiven wie oben nur parallele "Kontrollrechnungen" durch, so spricht man von einer separaten

Codierung. Sie besteht grob gesprochen in einer parallelen, modularen Rechnung. Eine dritte Möglichkeit, bei der man ohne zusätzliche arithmetische Prozessoren auskommt, ist eine direkte Codierung, welche redundante Information erzeugt, die der Fehlererkennung dient. Die einfachste Methode in dieser Hinsicht ist die Multiplikation mit einem festen Faktor g. Sind n_1, n_2 ganze Zahlen, so gilt $gn_1 + gn_2 = g\,(n_1 + n_2)$ und dieser Gleichung muss jede Codierung genügen, die Additionsfehler zu erkennen gestattet. Einen Fehler erkennen wir, wenn nach vollzogener Addition das Resultat nicht den Rest Null bei Division durch g ergibt. Überlegungen dieser Art hat wohl Garner [22], in einer leider wenig beachteten Arbeit, zum ersten Mal angestellt. Im Kapitel 1 verallgemeinern wir alles auf beliebige kommutative Ringe mit Einselement. Ein non-separater Restklassencode lässt sich dann als isomorphe Einbettung der additiven Gruppe eines Ringes in einen geeigneten zweiten Ring deuten, wobei das Bild ein Ideal ist. Fehler erkennt man durch Übergang zum Restklassenring. Für einen Restklassenring $\mathbb{Z}_m$ ist ein AN-Code danach eine Abbildung

$$\lambda_g : \mathbb{Z}_m^+ \longrightarrow \mathbb{Z}_{mg}^+$$

mit $\lambda_g(\bar{n}) = \overline{ng} = \overline{n}\,\overline{g}$. Setzen wir m = 0, so ist es gerade die vorhin diskutierte Codierung. Will man Fehler nicht nur erkennen, sondern auch korrigieren, so müssen sie "gewogen" werden, d.h. mathematisch gesprochen, es muss eine Fehlernorm auf den betrachteten Ringen eingeführt werden. Was ist nun eine Fehlernorm? Im Kapitel 2 geben wir die Antwort: eine k-Pseudobewertung, das ist eine verallgemeinerte Pseudobewertung. Pseudobewertungen sind schon lange bekannt, sie wurden von Mahler [38 - 41] ausführlich untersucht, während k-Pseudobewertungen unter dem Namen Pseudobewertungen "de pas fini" im Anschluss an Szipro [64] erst in neuerer Zeit von Sangare [60] untersucht wurden. Im Gegensatz zu diesen Autoren müssen wir voraussetzen, dass der Wertebereich der Fehlernorm natürliche Zahlen sind. Damit werden jedoch alle Ergebnisse, die sich auf topologische Argumente stützen trivial, so sind z.B. alle Fehlernormen trivialerweise

topologisch äquivalent. Wir bauen deshalb eine für unsere Zwecke geeignete Theorie auf. Zunächst zeigen wir, wie man eine Norm auf einen Faktorring fortsetzt. Dies ist wichtig, weil Computer nicht im Ring $\mathbb{Z}$ rechnen, sondern in $\mathbb{Z}_m$ mit $m = 2^n$ oder $2^n \pm 1$. In Abschnitt 2.2 leiten wir hinreichende Bedingungen für Fehlerkorrektur und Fehlererkennung in Ringen mit einer Norm her. Wie wir schon wissen, bilden die Codepunkte ein Ideal in einem geeigneten Ring, auf dem jetzt eine Norm definiert ist. Mit einem solchen Code ist es möglich, alle Fehler vom Gewicht (Gewicht und Norm sind Synonyme) $[D_{min} - 1/2]$ zu korrigieren, D_{min} ist die Minimaldistanz der Codepunkte bezüglich der von der Norm induzierten Metrik. Wie man leicht nachweist, ist D_{min} gleich der minimalen Norm aller Punkte des Ideals. Äquidistant heisst der Code, wenn alle Codepunkte gleiches Gewicht haben. Bisher haben wir über Ringe mit einer Norm gesprochen, ohne zu wissen wie wir uns eine solche Norm eventuell verschaffen können. Besitzt die additive Gruppe des Ringes R ein erzeugendes System S mit $S \neq R^+$, so haben wir in Satz 16 eine einfache Prozedur um eine nicht-triviale Norm zu erzeugen. Im Beispiel $R = \mathbb{Z}$ und $S = \{1\}$ ist es der absolute Betrag. Für die Anwendungen ist es viel wichtiger, Algorithmen zu finden, die es gestatten bei vorgegebener Norm $\|\ \|$ (auf R) und distinktem Ideal $\mathfrak{g}$ (in R) D_{min} zu bestimmen. Dazu ist es nötig, sich genauer mit der Struktur einer Norm zu beschäftigen. Unser Ziel erreichen wir über eine Äquivalenzrelation, deren Klassen sich als Orbits einer Gruppe, die auf R operiert, charakterisieren lassen. In der Bemerkung nach Lemma 26 skizzieren wir einen Algorithmus, der die gestellte Aufgabe in allen praktisch wichtigen Fällen löst. In Satz 26 formulieren wir alles für AN-Codes und erhalten eine weitgehende Verallgemeinerung des Ansatzes von Tsao-Wu [66] . Anknüpfend an den Begriff der vollständigen Folge bei Brown [7] greifen wir die Frage nach der Existenz nicht-trivialer Normen für $R = \mathbb{Z}$ erneut auf. Als Folgerung aus unseren Überlegungen ergibt sich in Satz 29 eine neue Ableitung für die in der Theorie der AN-Codes ausschliesslich benutzten Normen $\|\ \|_q$ $(q \geq 2)$. Weitere Fragen von z.Z. rein theoretischem Interesse, welche

unser Ansatz involviert, werden in den Bemerkungen auf Seite 26 gestreift. In Kapitel 3 beschäftigen wir uns ausschliesslich mit dem Ring der ganzen Zahlen. Wir geben die Motivation für die übliche Definition der Fehlernorm $\| \|_q$ und leiten in den Abschnitten 3.1-3.2 alle bekannten und einige neue Eigenschaften her. Insbesondere die kanonische NAF- bzw. GNAF-Darstellung nach Reitwiesner [58] und Clark/Liang [14]. Satz 42 und Bemerkung c. auf Seite 36 bilden später in 4.2 die Grundlage einer neuen Technik zur Abschätzung von D_{min}. Mit Satz 39 gewinnen wir den Anschluss an die abstrakten Untersuchungen in Kapitel 2, er sagt aus: die Norm $\| \|_q$ ist für $q = 2$ eine Pseudobewertung, für $q > 2$ eine 2-Pseudobewertung auf $\mathbb{Z}$. Die hinreichende Bedingung aus Satz 10 (2.2) für die Fehlerkorrektur ist nach Satz 44 auch notwendig. Aus Satz 46 folgt, es gilt in der Norm $\| \|_q$ stets $D_{min} \leq 2$ für jedes Ideal in $\mathbb{Z}$. Damit haben wir die Motivation, um die Funktion $M_q(g, d)$ in Definition 21 einzuführen. Ihr Wert ist die kleinste natürliche Zahl $n > 0$ mit der Eigenschaft $\| gn \|_q < d$, d.h. für alle $x \in (0, n-1]$ gilt $\| gx \|_q \geq d$.
Die Kenntnis des Verlaufs von $M_q(g, d)$ scheint zunächst ohne praktischen Wert zu sein, da ein Computer ja in $\mathbb{Z}_m$ ($m > 0$) und nicht in $\mathbb{Z}$ arbeitet. Doch Lemma 64 im Abschnitt 3.4 erlaubt es in den wichtigen Fällen $m = q^l \pm 1$ alle Ergebnisse zu übernehmen. Im Unterabschnitt 3.3.1 wird $M_2(g,3)$ berechnet ($d = 0, 1, 2$ ist trivial). Die Sätze von Brown (Satz 52) und Peterson (Satz 54) sind die ersten Resultate über AN-Codes, sie stammen aus den Jahren 1960/61. Es werden einige Verschärfungen angegeben. Werte von $M_q(g, 3)$ für $q > 2$ hat zuerst Gritsenko [26] 1969 publiziert, allerdings sind seine Sätze von recht speziellem Charakter. In 3.3.2 verallgemeinern wir in Satz 57 einige Sätze, die Neumann/Rao [47] 1975 gefunden haben, in Satz 58 einen Ansatz von Gritsenko l.c. und in Satz 59 einen Ansatz von Dynkin/Kimelfeld [20] . Mit Abschnitt 3.4 wenden wir uns den AN-Codes $\lambda_g : \mathbb{Z}_m^+ \longrightarrow \mathbb{Z}_{mg}^+$ zu, die z.Z. allein praktisches Interesse beanspruchen können. Ausgehend von der Norm $\| \|_q$ auf $\mathbb{Z}$ wissen wir aus Kapitel 2 bereits, wie sie zu einer Norm $\| \|_{q(m)}$ auf $\mathbb{Z}_m$ fortgesetzt werden kann. Wählt man $m = q^l \pm 1$, q^l so lässt sich diese Norm anders und einfacher definieren (Definition 25).

Der Herleitung dieses äußerst wichtigen Zusammenhanges ist Abschnitt 3.4 fast völlig gewidmet (das Analogon zu Satz 44 ist Satz 66). Im binären Fall $q = 2$ ist diese Beziehung bekannt (vgl. Massey/Garcia [44]), allgemein haben Clark/Liang [15] ähnliche Ergebnisse erzielt. Kapitel 4 ist dem Aufbau der Theorie der zyklischen Codes ($mg = q^l - 1$) für $q \geq 2$ gewidmet. Im binären Fall hat Tsao-Wu [66] einen Ansatz entwickelt, dessen Ausbau Massey/Garcia l c. beschreiben. Die grösste Schwierigkeit bietet bei der Verallgemeinerung auf $q > 2$ die Abschätzung bzw. exakte Berechnung von D_{min}. Abschnitt 4.1 ist von stark technischem Charakter, die Darstellung in dieser Form ist neu. Durch einen einfachen Trick (Satz 71) wird der sonst übliche unnatürliche Weg über periodische q-adische Brüche vermieden. Der wichtige Satz 79 entpuppt sich zurückblickend als einfache Folgerung aus der abstrakten Theorie (Satz 26). Wie schon erwähnt, bilden Satz 42 und eine Bemerkung aus 3.2 die Grundlage für eine neue Technik zur Abschätzung von D_{min}. Als Hilfsmittel benutzen wir zwei Sätze von Stoneham [62,63] über die Verteilung von Ziffernblöcken in der q-adischen Darstellung rationaler Brüche $\frac{x}{p^n}$ (p Primzahl). In Satz 90 und Satz 91 werden obere und untere Schranken für D_{min} angegeben unter den Voraussetzungen $mg = q^l - 1$, $m = p^n$ und q ist primitive Wurzel modulo p^2. Die Formel in Satz 90 lässt sich, wenn man die Theorie der Totative benutzt, in manchen Fällen auswerten, so dass sich geschlossene Ausdrücke ergeben (Satz 92, 93 und die Corollare). In 4.4 wird D_{min} unter der angeführten Voraussetzung exakt bestimmt. Lassen wir die Forderung q primitives Element modulo p^2 fallen, so können wir noch Aussagen wie in Satz 95 und Satz 96 machen. Satz 96 ist von grosser Allgemeinheit, es steht zu vermuten, dass unter den schwachen Voraussetzungen keine Verbesserung mehr möglich ist. Auf dem gewiesenen Wege ist es vielleicht möglich, weitere Abschätzungen zu gewinnen. Im nächsten Abschnitt (4.3) verallgemeinern wir einen Ansatz, der bei $q = 2$ schon längere Zeit dazu dient, für D_{min}, wenigstens in speziellen Fällen, den exakten Wert zu finden (siehe Massey/Garcia l.c.) Eine ähnliche Verallgemeinerung haben vor uns schon Clark/Liang [15] skizziert (es fehlen z.T. die

Beweise). Hauptergebnis ist Satz 106, für den sich, obwohl er im binären Fall häufig benutzt wird (z.B. Rao [54]), nirgends ein Beweis findet. Jetzt sind wir in der Lage, unter gewissen Voraussetzungen über m und q in den Sätzen, Lemmata, Corollaren 110 - 120 D_{min} zu berechnen. Abgesehen von Satz 110 gelingt es für $q > 2$ in dieser Arbeit zum ersten Mal. Die Berechnungen für $q = 2$ hat zuerst Tsao-Wu [66] vorgenommen, sie sind recht verwickelt und umfangreich. Unsere Technik über die Theorie der Totative zu gehen, stellt auch im binären Fall eine erhebliche Vereinfachung dar. In den Sätzen 113 und 114 werden zwei neue Klassen äquidistanter Codes entdeckt und so eine Vermutung von Massey/ Garcia (l.c. pp. 305 unten) widerlegt. Wir führen die Begriffe f(ast) - äquidistanter und a(symptotisch) - äquidistanter Code ein und zeigen in den Corollaren 115.1, 120.2 die Existenz derartiger A_N-Codes. Die Sätze 121 - 123 werden in Abschnitt 4.4 gebraucht, in Corollar 122.1 (ebenso Lemma 124) wird D_{min} nach oben abgeschätzt. Durch unsere Untersuchungen ist es auch für $q > 2$ gelungen AN-Codes mit hohem D_{min} zu finden, die es also gestatten, Fehler von grossem Gewicht zu korrigieren. Wie eine simple Rechnung zeigt, besitzen sie eine niedrige Rate und sind somit unwirtschaftlich. Andererseits besitzen die perfekten Codes (dichteste Kugelpackung!) der Sätze 69, 70 hohe Rate, jedoch ist $D_{min} = 3$. Es ist deshalb von praktischer Bedeutung, mittels geeigneter Algorithmen AN-Codes mit hohem D_{min} und wenigstens mittlerer Rate aufzufinden. Das lässt sich nach Chien/ Hong/Preparata [12] im Fall $q = 2$ durch systematische Suche in einer geeigneten "Umgebung" der AN-Codes mit hohem D_{min} erreichen. Wir verallgemeinern [12] in Abschnitt 4.4 auf $q \geq 2$. Abschließend sei betont, dass,wie wir gezeigt haben, zwar eine Verallgemeinerung der Theorie der zyklischen AN-Codes von $q = 2$ auf $q \geq 2$ möglich ist, aber es besteht ein wichtiger Unterschied. Ist $q > 2$ und genügend gross, so können die Berechnungen in 4.3 (4.4) in einem konkreten Fall eventuell nicht mehr ausgeführt werden. Aus diesem Grund wird es immer nützlich sein, D_{min} wie in 4.2 abzuschätzen.

Der Verfasser möchte Herrn Professor Dr. H.-J. Töpfer an dieser Stelle seinen Dank aussprechen, für die Möglichkeit, diese Untersuchungen im Rahmen des Teilbereichs D/M des Hahn-Meitner-Instituts für Kernforschung durchzuführen.

Inhaltsverzeichnis

	Seite
Einleitung	- 9
Inhaltsverzeichnis	- 1
Kapitel 1 Fehlercodes für arithmetische Operationen	ø
1.1 Separate Codes	1
1.2 Non-separate Codes	3
1.3 Systematische Codes	7
1.4 Implementierung von Restklassencodes	8
Kapitel 2 Ringe mit arithmetischer Norm	10
2.1 Definition und Eigenschaften der Norm	10
2.2 Fehlerkorrektur in Ringen mit einer Norm	13
2.2.1 Rate und Redundanz	15
2.3 Eigenschaften der ganzzahligen Norm	16
Kapitel 3 Fehler in der Integerarithmetik von Computern	28
3.1 Normen auf dem Ring der ganzen Zahlen	29
3.2 Eigenschaften der Norm $\|\|_q$	32
3.3 Fehlererkennung bei unbeschränkter Integer-arithmetik	37
3.3.1 Berechnung von M_2 (g, d)	42
3.3.2 Berechnung von M_q (g, d) für $q \geq 2$	45
3.4 Fehlererkennung und -korrektur in der modularen Arithmetik	50
Kapitel 4 Theorie der zyklischen Codes	56
4.1 Zyklische Permutationen	56
4.2 Abschätzung von D_{min}	67
4.3 Der zyklische GNAF	76
4.4 Berechnung von D_{min} für spezielle Werte von m	87
4.5 Zyklische Codes hoher Rate	106
Symboltabelle	116
Literaturverzeichnis	119

Kapitel 1

Fehlercodes für arithmetische Operationen

Die arithmetischen Operationen, welche uns interessieren, sollen Addition und Multiplikation sein, in einem fest vorgegebenen kommutativen Ring mit Einselement 1 (Verwechslungen mit der natürlichen Zahl 1 sind kaum möglich). Mit der Arithmetik in R beherrschen wir auch zugleich die Arithmetik in $R/\mathfrak{a}$, wo $\mathfrak{a}$ ein Ideal in R ist. Es ist sinnvoll, alle Überlegungen für Ringe $\overline{R} = R/\mathfrak{m}$ durchzuführen, wo $\overline{R}$ im Fall $\mathfrak{m} \neq (o)$ sogar als endlich vorausgesetzt werden kann. Denn in der Praxis ist $R = \mathbb{Z}$ ein unendlicher Ring, es wird aber in $\mathbb{Z}_m$ ($m = 2^n$ oder $2^n - 1$) gerechnet.

Die arithmetischen Operationen in R sollen von einem "Gerät" ausgeführt werden, das wir als arithmetische Einheit oder auch, falls uns nur die Addition interessiert, als Addierer bezeichnen. Diese arithmetische Einheit arbeitet nicht fehlerfrei, die Menge der relevanten Fehler sei $E \subset \overline{R}$, es soll stets gelten $\emptyset \in E$.
Die Aufgabe, welche wir uns stellen, besteht darin, Methoden zu finden, welche es gestatten, Fehler aus E zu erkennen und/oder zu korrigieren, d.h. es gilt $E = E_c \cup E_d$ und $E_c \cap E_d = \{0\}$, wobei E_c die Menge der zu korrigierenden, E_d die Menge der zu entdeckenden Fehler ist. Aus $E_c \cap E_d \supset \{0\}$ (echt umfassend) würde folgen, dass eine Prozedur zur effektiven Durchführung von Fehlererkennung und Fehlerkorrektur nicht-deterministisch arbeiten müsste, d.h. durch keinen Algorithmus realisiert werden könnte. Fehlercodes für arithmetische Operationen setzen sich zusammen aus einer Codierung der Elemente von $\overline{R}$ und einem Kontrollcode, der nach vollzogener Operation festzustellen gestattet, ob eventuell ein Fehler aufgetreten ist.

Definition 1 Ein Kontrollcode zur Basis $\{\mathfrak{y}_i\}_{i \in J}$ für arithmetische Operationen in einem Ring $\overline{R}$, wo $\mathfrak{y}_i \subset K$ für alle $i \in J$ Ideale im Ring K sind, ist eine Familie $\{\gamma_i\}_{i \in J}$ von Abbildungen

$$\gamma_i : K \longrightarrow K / \mathfrak{y}_i$$

mit $K = \overline{R}$ oder $\overline{R}$ ist durch einen Isomorphismus λ,

$$\lambda : \overline{R} \xrightarrow{+} K$$

der additiven Gruppe $\overline{R}^+$ von $\overline{R}$, in K eingebettet. Dabei ist $K = R/\mathfrak{m}$ ein geeigneter Faktorring von R.

Fehlercodes, deren Kontrollcodes durch Definition 1 beschrieben werden, heissen aus verständlichen Gründen Restklassencodes. - Jedem Ideal $\bar{\mathfrak{y}}$ in $\overline{R}$ entspricht genau ein Ideal $\mathfrak{y} \supset \mathfrak{m}$ in R. Wir werden uns diese Zuordnung zunutze machen und stets die entsprechenden Ideale in R statt der Ideale in $\overline{R}$ betrachten. Ist R ein Hauptidealring, so folgt $\mathfrak{y} = (g)$, $\mathfrak{m} = (m)$, $(g, m \in R)$ und $g \mid m$. -
In den folgenden Abschnitten geben wir eine kurze Übersicht der wichtigsten Restklassencodes zur Fehlererkennung, die zur Zeit untersucht werden.

1.1 Separate Codes

Definition 2 Ein separater Mono-Restklassencode ist eine Abbildung

$$\mathrm{id}_{\overline{R}} \times \gamma : \overline{R} \longrightarrow \overline{R} \oplus \overline{R}_{\mathfrak{y}}$$

$$\mathrm{id}_{\overline{R}} \times \gamma\,(\bar{r}) = (\bar{r}, \gamma(\bar{r})) \quad (\bar{r} \in \overline{R})$$

und γ ist der kanonische Homomorphismus

$$\gamma : \overline{R} \to \overline{R}_{\mathfrak{y}} = R/\mathfrak{y} \simeq \overline{R}/\mathfrak{y}/\mathfrak{m} \quad (\mathfrak{y} \supset \mathfrak{m})$$

Dass γ notwendig ein Homomorphismus sein muss, folgt aus der Forderung, dass die Fehlerkontrolle durch Vergleich von $\gamma(\bar{r}_1 + \bar{r}_2)$ $(\bar{r}_1, \bar{r}_2 \in \overline{R})$ mit $\gamma(\bar{r}_1) + \gamma(\bar{r}_2)$ bzw. von $\gamma(\bar{r}_1 \cdot \bar{r}_2)$ mit $\gamma(\bar{r}_1) \cdot \gamma(\bar{r}_2)$ erfolgt (bei fehlerfreier Operation muss Gleichheit gelten). Es wird vorausgesetzt, dass die arithmetischen Operationen in $\overline{R}$ und $\overline{R}_{\mathfrak{y}}$ von verschiedenen arithmetischen Einheiten ohne irgendwelche gegenseitige Beeinflussung durchgeführt werden. Da die arithmetische Einheit, welche die Arithmetik in $\overline{R}_{\mathfrak{y}}$ durchführt, nicht fehlerfrei arbeitet, muss man zumindest sicher sein, dass Fehler mit einer geringeren Wahrscheinlichkeit auftreten als in der arithmetischen Einheit für $\overline{R}$ und es sollte gelten $\gamma(E) \cap F = \{0\}$, wo $F \subset \overline{R}_{\mathfrak{y}}$ die Menge der möglichen Fehler ist.

Definition 3 Das Syndrom eines separaten Mono-Restklassencodes ist die Abbildung

$$S : \overline{R} \oplus \overline{R}_g \rightarrow \overline{R}_g$$

definiert durch

$$S(\overline{r}, \overline{r}_1) = \overline{\overline{r - r_1}} = \overline{r} - \overline{r}_1 \in \overline{R}_g$$

Das Element $S(\overline{r}, \overline{0})$ heisst Syndrom von $\overline{r} \in \overline{R}$.

Wegen $g \nmid m$ ist S eine Abbildung und es gilt die angegebene Beziehung. Ist als Ergebnis einer arithmetischen Operation ein Fehler in $\overline{R}$ aber nicht in $\overline{R}_g$ aufgetreten, so hat man

$$S(\overline{r} + \overline{e}, \overline{r}) = \overline{e} \in \overline{R}_g$$

wo $\overline{e} \in E \subset \overline{R}$. Aus dieser Überlegung folgt schon der

Satz 1 Ein separater Mono-Restklassencode mit $E = E_c \cup E_d \subset \overline{R}$ kann genau dann alle Fehler aus E_c korrigieren und alle Fehler aus E_d entdecken, wenn kein $\overline{e}_1 \in E_c$ existiert, so dass gilt

$$S(\overline{e}_1, \overline{0}) = \overline{e}_1 = \overline{e}_2 = S(\overline{e}_2, \overline{0})$$

für ein $\overline{e}_2 \in E \setminus \{0\}$.

Ist nun $\overline{R} = \mathbb{Z}_m$ und $\overline{n} \in \mathbb{Z}_m$ wird im Zahlensystem zur Basis q geschrieben, so muss man fordern $\mathbb{Z}_g \nmid \overline{q^i} \neq 0$ für alle i, da sonst ein Fehler im Koeffizienten $\mathcal{L}_i$ nicht entdeckt werden könnte. Durch (q, g) = 1 lässt sich dies stets erreichen. Zusammengefasst hat man nach Garner [22] .

Satz 2 Hinreichend für die Existenz eines separaten Mono-Restklassencode mit Kontrollcode zur Basis g ist: $g \mid m$ und (g, q) = 1, wenn q die Basis für eine Darstellung der $\overline{n} \in \mathbb{Z}_m$ ist.

Bemerkung Gilt (g, m) ≠ 1, so muss man $\mathbb{Z}_m$ erweitern zu $\mathbb{Z}_{m'}$ mit $m' > m$ und $g \mid m'$. Wichtig sind die Fälle $m = q^n$ und $m = q^n - 1$. Im ersten Fall müssen wir erweitern, denn aus (g, q) = 1 folgt $g \nmid q^n$. Im zweiten Fall ist $g = q - 1$ eine Lösung und für gerades n auch $g = q + 1$.

Definition 4 Ein separater Multi-Restklassencode ist eine

Abbildung

$$\mathrm{id}_{\overline{R}} \times \gamma_1 \times \cdots \times \gamma_l : \overline{R} \longrightarrow \overline{R} \oplus \overline{R}_{\nu_1} \oplus \cdots \oplus \overline{R}_{\nu_l}$$

$$\mathrm{id}_{\overline{R}} \times \gamma_1 \times \cdots \times \gamma_l (\overline{r}) = (\overline{r}, \gamma_1(\overline{r}), \ldots \gamma_l(\overline{r}))$$

und die γ_i ($i = 1, \ldots, l$) sind die kanonischen Homomorphismen

$$\gamma_i : \overline{R} \longrightarrow \overline{R}_{\nu_i} = R/\nu_i \simeq \overline{R}/\nu_i/\mathfrak{m} \quad (\nu_i \supset \mathfrak{m})$$

Weiter gilt $\nu_i + \nu_j = R$ für $i \neq j$, d.h. die Ideale sind paarweise teilerfremd.

Bemerkung Mit dem Chinesischen Restsatz folgt aus Definition sofort

$$R/\bigcap_i \nu_i \simeq \prod R/\nu_i$$

und wegen $\bigcap \nu_i = \nu_1 \cdot \nu_2 \cdot \cdots \cdot \nu_l = \nu$ können wir die direkte Summe $\overline{R} \oplus \overline{R}_\nu$ schreiben. Algebraisch besteht demnach zwischen Mono- und Multi-Restklassencodes kein Unterschied. Er besteht nur in der Implementation, da jeder Komponente des direkten Produktes eine separate arithmetische Einheit entspricht. Es können dann auch Fehler der Kontrolleinheiten erkannt und korrigiert werden. Das Syndrom für separate Multi-Restklassencodes ist eine entsprechende Verallgemeinerung von Definition 3. Für weitere Einzelheiten siehe Garcia [21], Rao/Garcia [53].

1.2. Non-separate Codes

Definition 4 Ein non-separater Restklassencode ist ein Isomorphismus

$$\lambda : \overline{R}^+ \longrightarrow K^+, \quad K = R/\nu$$

wo $\mathrm{Im}\lambda = \nu_\nu$ ein Ideal in K ist.
Es ist sinnvoll, $\nu = \mathfrak{m} \cdot \nu_\nu$ zu wählen (im Fall $R = \mathbb{Z}$ werden wir die Existenz eines solchen Ideals ν_ν zeigen). Dann gilt $K/\mathfrak{m} \simeq \overline{R}$, d.h. der Ring K ist genügend gross.

Als Kontrollcode bietet sich der kanonische Homomorphismus

$$\delta : K \longrightarrow K/\nu_\nu \simeq \overline{R}_\nu$$

an. Das Syndrom ist in diesem Fall gleich dem Kontrollcode.

Es gilt E⊂K und um einen Fehler überhaupt entdecken zu können muss gelten $E \cap \mathfrak{y} = \{0\}$. Die Summe $\mathfrak{y} + E$ ist also direkt. Durchläuft E ein vollständiges Restsystem modulo $\mathfrak{y}$, so gilt $K = \mathfrak{y} + E$ und $|E| = |R/\mathfrak{y}|$, der Code wird bei bestehen dieser Gleichung perfekt genannt.

Satz 3 Ein non-separater Restklassencode mit $E = E_c \cup E_d \subset K$ kann genau dann alle Fehler aus E_c korrigieren und alle Fehler aus E_d entdecken, wenn kein $e_1 \in E_c$ existiert mit $\zeta(e_1) = \zeta(e_2)$ für ein $e_2 \in E \setminus \{0\}$.

Sind die Voraussetzungen von Satz 3 erfüllt, so lässt sich eine Funktion

$$T : \overline{R}_{\mathfrak{y}} \longrightarrow K \cup \{\varepsilon\} \quad (\varepsilon \notin K)$$

definieren,

$$T(\overline{r}) = \begin{cases} e, \text{ wenn } \zeta(e) = \overline{r} \text{ und } e \in E_c \\ c \in E_d \setminus \{0\} \text{ falls } e \in E_d \setminus \{0\} \text{ mit } \zeta(e) = \overline{r} \text{ existiert} \\ \varepsilon \text{ sonst} \end{cases}$$

Wir können dann einen Algorithmus angeben, der es gestattet, nach einer arithmetischen Operation Fehler aus E zu entdecken bzw. zu korrigieren.

S0 : R := R_1 OP R_2 ;
S1 : If $\zeta(R) = \emptyset$ or $T(\zeta(R)) = \varepsilon$ then goto STOP;
S2 : If $T(\zeta(R)) \in E_d$ then goto ERROR;
S3 : R := R - $T(\zeta(R))$;

Mit OP bezeichnen wir die Operation (Multiplikation oder Addition), R_1, R_2 sollen Elemente aus $\mathfrak{y}$ entsprechen.

In einem Hauptidealring ist wieder $\mathfrak{y} = (g)$, $\mathfrak{m} = (m)$ und weiter $(m)(g) = (mg)$. Spezialisieren wir auf $R = \mathbb{Z}$, $\overline{R} = \mathbb{Z}_m$, $K = \mathbb{Z}_{mg}$ so ist $\lambda : \mathbb{Z}_m^+ \to \mathbb{Z}_{mg}^+$ durch $\lambda(\overline{n}) = \overline{ng}$ $(\overline{n} \in \mathbb{Z}_m)$ definiert und dies ist auch die im wesentlichen einzige Möglichkeit, da die additive Gruppe von $\mathbb{Z}_m$ zyklisch ist und ein erzeugendes Element wieder auf ein solches abgebildet wird. Wie man sich leicht überlegt, lassen sich alle Erzeugenden des Ideals $(\overline{g})$ in $\mathbb{Z}_{mg}$ $\overline{ag}$ mit $(a,m) = 1$ schreiben. Es gibt demnach $\varphi(m)$ verschiedene Isomorphismen $\lambda : \mathbb{Z}_m^+ \longrightarrow \mathbb{Z}_{mg}^+$ die unseren Bedingungen genügen. Wie im Fall der separaten Codes fordern wir $(q, g) = 1$. Wichtig ist der

Fall $mg = q^n - 1$, d.h. $g \mid q^n - 1$; sollte $mg < q^n - 1$ gelten, so kann man eine additive Korrektur $B = (q^n - 1) - mg$ anbringen. Codes die durch $\lambda(\overline{m}) = \overline{mg}$ definiert sind, werden nach Brown [6] AN-Codes, bzw. bei additiver Korrektur $\lambda(\overline{m}) = \overline{mg + B}$, AN + B-Codes genannt. Betrachten wir den Sonderfall $\lambda: R^+ \longrightarrow R^+$, und fordern, dass λ ein (additiver) Endomorphismus sein soll, so wird durch $\lambda_g(n) = ng$ $(n, g \in R)$ ein solcher Endomorphismus definiert und die Zuordnung $\Phi : R \longrightarrow \mathrm{End}\, R^+$ definiert durch $\Phi(g) = \lambda_g$ ist ein (Ring-) Isomorphismus, der R auf einen Unterring des Endomorphismenringes der additiven Gruppe von R abbildet. Im Fall $R = \mathbb{Z}_m$ ist Φ sogar surjektiv, was zeigt, dass die AN-Codes sozusagen die einzigen arithmetischen non-separaten Codes sind.

Beispiele a. $q = 2$, $g = 3$, $m = 16$, $K = \mathbb{Z}_{48}$

$E_d = \{\pm 2^i \mid i \geq 0\} \cup \{0\}$, $2^i \equiv (-1)^i \bmod 3$

$E_c = \{0\}$

$(g) = \{0, 3, 6, \ldots, 45\} \subset \mathbb{Z}_{48}$

$E \cap (g) = \{0\}$

$\delta : \mathbb{Z}_{48} \longrightarrow \mathbb{Z}_{48} / (3) \cong \mathbb{Z}_3$ Jeder "einfache" Fehler kann erkannt werden.

b. $q = 10$, $g = 11$, $m = 0$, $K = \mathbb{Z}$

$E_d = \{\pm \alpha 10^i \mid i \geq 0 ; \alpha = 0, 1, \ldots, 9\}$, $\alpha 10^i \equiv \alpha(-1)^i \bmod 11$

$E_c = \{0\}$

$(g) = \{\pm \beta \cdot 11 \mid \beta \geq 0\} \subset \mathbb{Z}$

$E \cap (g) = \{0\}$

$\delta : \mathbb{Z} \longrightarrow \mathbb{Z} / (11) = \mathbb{Z}_{11}$ Jeder "einfache" Fehler kann erkannt werden.

Non-separate Codes können als spezielle separate Codes aufgefasst werden, wenn man $K = \overline{R} \oplus \overline{R}_{\vartheta}$ wählt.
Ein wichtiger Zusammenhang zwischen separaten und non-separaten Restklassencodes hat zuerst Garcia [21] bemerkt. Wir formulieren ihn als Satz 4 und verallgemeinern auf beliebige Ringe.

Satz 4 Gegeben ein non-separater Code, der sämtliche Fehler aus $E_c \subset K$ korrigieren kann und es gelte $\vartheta = \prod_{i=1}^{\ell} \vartheta_i$, wobei die ϑ_i

paarweise teilerfremde Idealeaus R sind (d.h. $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$). Dann gibt es einen Multi-Restklassencode

$$K \longrightarrow K \oplus \bar{R}_{\mathfrak{a}_1} \oplus \dots \oplus \bar{R}_{\mathfrak{a}_l}$$

der für alle Elemente aus E_c ein eindeutig bestimmtes Syndrom liefert, d.h. alle Fehler aus E_c korrigieren kann.
Umgekehrt sei ein separater Multi-Restklassencode

$$\bar{R} \longrightarrow \bar{R} + \bar{R}_{\mathfrak{y}_1} \oplus \dots \oplus \bar{R}_{\mathfrak{y}_l}$$

gegeben, der alle Fehler aus $E_c \subset \bar{R}$ korrigieren kann. Dann kann der zugeordnete non-separate Restklassencode mit $\mathfrak{a} = (\prod \mathfrak{y}_i) \cdot m = \mathfrak{y} \cdot m$ ebenfalls alle Fehler aus E_c korrigieren.

Beweis Im wesentlichen folgt alles aus der Gleichung

$$\prod_{i=1}^{e} \mathfrak{a}_i = \bigcap_{i=1}^{e} \mathfrak{a}_i \qquad (e \geq 1)$$

für paarweise teilerfremde Ideale $\mathfrak{a}_i$ und dem Chinesischen Restsatz.
Es dürfte klar sein, wie diese Aussage für $\mathbb{Z}_m$ zu formulieren ist. Man beachte: Fehler dürfen nur in der eigentlichen arithmetischen Einheit nicht in den Kontrolleinheiten auftreten. Die Voraussetzung über die Zerlegung von $\mathfrak{y}$ in teilerfremde Ideale ist in Hauptidealringen erfüllt.

Beispiel $K = \mathbb{Z}_{mg}$ mit $mg = 2^{35} - 1$ und $g = 31 * 127$

$$\lambda : \mathbb{Z}_m^+ \longrightarrow \mathbb{Z}_{mg}^+$$

Wie wir noch zeigen werden, kann dieser AN-Code alle Fehler aus $E = \{\pm 2^i \mid i \geq 0\} \subset K$ korrigieren. Aus Satz 4 folgt dann, dass der Bi-Restklassencode

$$\mathbb{Z}_{mg} \longrightarrow \mathbb{Z}_{mg} \oplus \mathbb{Z}_{31} \oplus \mathbb{Z}_{127}$$

die Korrektur der Fehler aus E gestattet.

1.3 Systematische Codes

Definition 5 Ein non-separater Code $\lambda : \overline{R}^{+} \longrightarrow K^{+}$ wird systematisch genannt, wenn gilt

$$\varkappa(\lambda(r)) = r \quad (r \in \overline{R})$$

wo $\varkappa : K \longrightarrow K/m \simeq \overline{R}$ der kanonische Homomorphismus ist.
Aus dieser Definition folgt notwendig

$$(1)\quad \lambda(r) = c_r + \varsigma_U(r) \quad (r \in \overline{R},\ c_r \in m)$$

$U \subset R$ ist ein Repräsentantensystem für die Elemente aus $R/m = \overline{R}$, d.h. zu jedem $r \in \overline{R}$ gibt es genau ein $u \in U$ mit der Eigenschaft $\overline{u} = r$. Dann ist die Abbildung

$$\varsigma_U : \overline{R} \longrightarrow K$$

durch $\varsigma_U(r) = \overline{u} \in K$
für alle $r \in \overline{R}$ definiert. Mittels ς_U ist $\overline{R}$ in K eingebettet.
Aus (1) folgt

$$\varphi \subset m + \varsigma_U(\overline{R})$$

Der Vorteil systematischer Codes liegt darin, dass die Verschlüsselung den ursprünglichen Wert "enthält". Wir müssen noch zeigen, dass systematische Codes existieren. Zu diesem Zweck und wegen der praktischen Bedeutung untersuchen wir den Fall $\overline{R} = \mathbb{Z}_m$, $K = \mathbb{Z}_{mg}$ genauer. Wie λ aussehen muss, wissen wir bereits. Als Repräsentantensystem $U \subset \mathbb{Z}$ wählen wir, wie üblich, die kleinsten positiven Reste. Daraus folgt unmittelbar

$$(2)\quad \lambda(1) = ag \equiv z \cdot m + 1 = h$$

mit $(a, m) = 1$ und $z \in \mathbb{Z}_g$. Die Kongruenz $xg \equiv 1 \bmod m$ besitzt unter der Voraussetzung $(g,m) = 1$ (sie folgt direkt aus (2)) genau eine Lösung. Durch die Forderung $z \in \mathbb{Z}_g$ ist dann h eindeutig bestimmt. Es gilt der

Satz 5 Notwendig und hinreichend für die Existenz eines systematischen Restklassencodes mit einem Kontrollcode zur Basis (g) ist $(g,m) = 1$.

Gilt $m > g$ (der praktisch sinnvolle Fall!), so hat man die Gleichheit $ag = h$ in (2). Wählen wir nun eine Darstellung zur Basis q für die Elemente aus $\mathbb{Z}$ und damit aus $\mathbb{Z}_m$ bzw. $\mathbb{Z}_{mg}$,

so empfiehlt es sich $m = q^k$ zu wählen (Voraussetzung: $(q,g) = 1$). Denn wie aus (2) zu erkennen ist, wird $n \in \mathbb{Z}_m$ dann auf $\lambda(n) = n \cdot z \cdot q^k + n \in \mathbb{Z}_{mg}$ abgebildet und wegen $n < q^k - 1$ kann n in der Darstellung von $\lambda(n)$ zur Basis q identifiziert werden.

Beispiel $m = 16$, $g = 3$, $q = 2$

$3x \equiv 1 \bmod 16$ ergibt als Lösung $x = 11$, d.h.

$$11 \cdot 3 = 2 \cdot 16 + 1 = h$$

Der systematische Code:

ø	⟷	øø øøøø
1	⟷	1ø øøø1
2	⟷	ø1 øø1ø
3	⟷	øø øø11
.		
.		
.		
14	⟷	ø1 111ø
15	⟷	øø 1111

1.4 Implementierung von Restklassencodes

Verfahren zum Erkennen und/oder Korrigieren von arithmetischen Fehlern müssen sich ohne grossen Aufwand implementieren lassen. Zum Einen aus Kostengründen, zum Anderen ist jede zusätzliche Ausrüstung um so fehleranfälliger je komplexer sie ist. Wir folgen der Dissertation von Garcia [21] .

1. AN-Codes

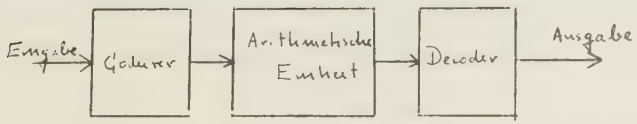
Eine mögliche Implementation könnte wie folgt aussehen:

(i) ein Codierer zur Verschlüsselung der Information (an);

(ii) ein Addierer,

(iii) ein Decoder, der das Ergebnis $a(n_1 + n_2) + e = m$ hernimmt, das Syndrom bestimmt und je nach Resultat weiter verfährt.

Diese Implementierung ist in Abb. 1 schematisch dargestellt.



2. Multi-Restklassencodes

Eine mögliche Form der Implementierung ist in Abb. 2 zu sehen. In der arithmetischen Einheit wird die Arithmetik modulo m ausgeführt in den k anderen Einheiten modulo g_i (i = 1, ..., k).

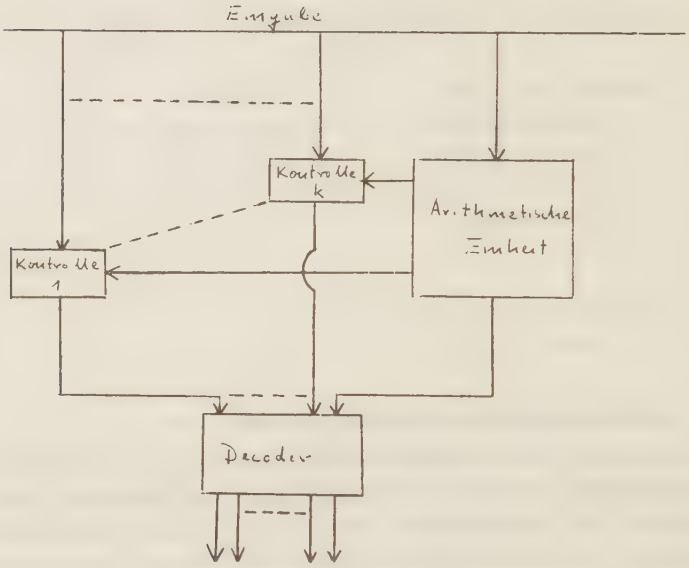


Abb. 2 Implementierung von Multi-Restklassencodes

3. Non-separate systematische Codes

Abb. 3 zeigt im Blockdiagramm eine mögliche Implementierung.

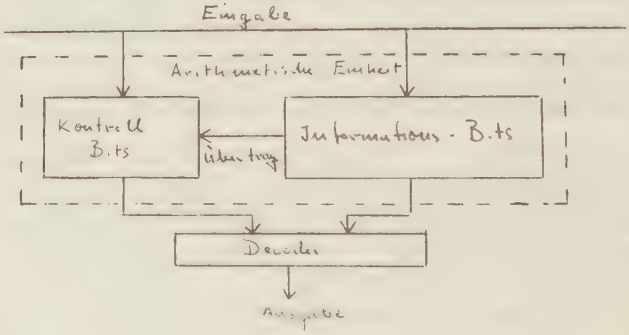


Abb. 3 Implementierung von non-separaten systematischen Codes

Kapitel 2

Ringe mit arithmetischer Norm

2.1 Definition und Eigenschaften der Norm

Definition 6 Eine Abbildung $\| \ \| : R \longrightarrow \mathbb{R}$ des Ringes R in die Menge der reellen Zahlen heisst k-Pseudobewertung ($k \geq 1$ ist eine reelle Zahl), wenn sie den folgenden Bedingungen genügt:

(AW∅) $\| r \| \geq 0 \quad (r \in R)$

(AW1) $\| r \| = 0 \Longleftrightarrow r = 0 \quad (r \in R)$

(AW2) $\| r_1 + r_2 \| \leq \| r_1 \| + \| r_2 \| \quad (r_1, r_2 \in R)$

(AW3) $\| r \| = \| -r \|$ für alle $r \in R$

(AW4) $\| r_1 r_2 \| \leq k \cdot \| r_1 \| \cdot \| r_2 \|$ für alle $r_1, r_2 \in R$

Gilt (AW2) in der stärkeren Form

(AW2') $\| r_1 + r_2 \| \leq \max (\| r_1 \| , \| r_2 \|)$ für alle $r_1, r_2 \in R$

so wird $\| \ \|$ eine nicht-archimedische k-Pseudobewertung genannt. Gilt in (AW4) die Gleichheit,

(AW4') $\| r_1 r_2 \| = k \cdot \| r_1 \| \cdot \| r_2 \|$ für alle $r_1, r_2 \in R$

so heisst $\| \ \|$ eine k-Bewertung. Ist $k = 1$, so spricht man von einer Pseudobewertung bzw. Bewertung. Eine k-Pseudobewertung werden wir auch kurz eine Norm auf R nennen.

Lemma 6 Sei R ein Ring mit einer k-Pseudobewertung, verschieden vom Nullring. Dann gilt:

(i) $\| r_1 - r_2 \| \leq \| r_1 \| + \| r_2 \|$ für alle $r_1, r_2 \in R$

(ii) $\| 1 \| \geq 1$ für eine Pseudobewertung, $\| 1 \| = 1$ für eine Bewertung

(iii) Jede k-Bewertung ist schon eine Bewertung, falls $\| \ \| (R) \subset \mathbb{N}$ gilt, oder wenn $\| 1 \| = 1$ ist.

(iv) Jeder Ring mit einer Bewertung ist ein Integritätsbereich.

(v) $\left| \| r_1 \| - \| r_2 \| \right| \leq \| r_1 - r_2 \|$

Bemerkung

a. Fordert man in Defintion 6 nur (AW1') $\| 0 \| = 0$, so bilden die $r \in R$ mit $\| r \| = 0$, wie man sich leicht überlegt, ein Ideal $\mathfrak{o}_0$ in R.

b. (AW2) und (AW3) kann man auch zusammenfassen als
(AW23) $\|r_1 - r_2\| \leq \|r_1\| + \|r_2\|$. Dann lässt sich $\|r\| = \|-r\|$ ableiten.

c. Nicht-archimedische k-Pseudobewertungen werden allgemein anders geschrieben:

(AWØ) $\|r\|_{NA} \in \overline{\mathbb{R}}$ $(r \in R)$

(AW1) $\|r\|_{NA} = \infty \Longleftrightarrow r = 0$ $(r \in R)$

(AW2) $\|r_1 + r_2\|_{NA} \geq \text{Min}(\|r_1\|_{NA}, \|r_2\|_{NA})$ $(r_1, r_2 \in R)$

(AW3) $\|r\|_{NA} = \|-r\|_{NA}$ $(r \in R)$

(AW4) $\|r_1 \cdot r_2\|_{NA} \geq \|r_1\|_{NA} + \|r_2\|_{NA} + \gamma (r_1, r_2 \in R, \gamma \in \mathbb{R})$

Dies wird erreicht, indem man $\|r\|_{NA} = -\log \|r\|$ für $r \in R$, $r \neq 0$ und $\|0\|_{NA} = \infty$ setzt ($\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$).

Beispiele

a. Jeder Ring besitzt die triviale Pseudobewertung:

$$\|r\|_0 = \begin{cases} 0 & \text{falls } r = 0 \\ 1 & \text{sonst} \end{cases} \qquad (r \in R)$$

b. Ist $\mathfrak{a} \subset R$ ein Ideal des Ringes, so ist

$$\|r\|_{\mathfrak{a}} = \begin{cases} 0 & \text{falls } r \in \mathfrak{a} \\ 1 & \text{sonst} \end{cases} \qquad (r \in R)$$

eine Pseudobewertung mit der Bedingung (AW1') (siehe oben).

c. Im Körper der rationalen Zahlen $\mathbb{Q}$ sei $\frac{r}{s}$ ein Bruch mit $r \neq 0$, $s > 0$ und $(r, s) = 1$. Zu fest vorgegebenem $q \geq 2$ existiert dann eine eindeutig bestimmte ganze Zahl $f \in \mathbb{Z}$ mit der Eigenschaft,

$$q^f \cdot \frac{r}{s} = \frac{r'}{s'}$$

wo $(r', s') = 1$, $(q, s') = 1$ und $q \nmid r'$ gilt.

Setzen wir nun

$$\left\| \frac{r}{s} \right\|_{q\text{-ad}} = q^f \text{ und } \|0\|_{q\text{-ad}} = 0$$

so ist $\|\ \|_{q\text{-ad}}$ eine Pseudobewertung von $\mathbb{Q}$ und für $q = p$ (p Primzahl) eine Bewertung. Diese Pseudobewertungen bzw. Bewertungen werden als q-adische Pseudobewertungen bzw. p-adische Bewertungen

von $\mathbb{Q}$ bezeichnet, sie sind nicht-archimedisch (siehe Mahler [41]).

d. Sei $\mathfrak{a}$ ein Ideal von R. Dann ist die Funktion,

$$\|\|_{\mathfrak{a}}: R \longrightarrow \overline{\mathbb{R}}$$

welche durch $\|r\|_{\mathfrak{a}} = \sup \{n \mid n \in \overline{\mathbb{N}},\ r \in \mathfrak{a}^n\}$ definiert ist eine nicht-archimedische Pseudobewertung von R. Solche Pseudobewertungen wurden von Rees ([55] , [56] , [57]) und anderen eingehend untersucht. k-Pseudobewertungen ergeben sich in diesem Zusammenhang als natürliche Verallgemeinerungen (siehe Szipro [64]). Daß k-Pseudobewertungen auch an sich interessant sind, zeigt die Arbeit von Sangare [60] .

Lemma 7 Jede Norm $\|\ \|$ auf einem Ring R induziert eine Metrik d, mittels

$$d(r_1, r_2) = \|r_1 - r_2\| \qquad (r_1, r_2 \in R)$$

und (R, d) ist ein metrischer Raum.

Beweis Man weist leicht nach, dass die Axiome für eine Metrik erfüllt sind.

Bemerkung Wie man leicht zeigt, sind Multiplikation und Addition stetige Operationen bezüglich dieser Metrik.

Definition 7 Eine Norm $\|\ \| : R \longrightarrow \mathbb{R}^+$ heisst ganzzahlig, wenn $\|r\| \in \mathbb{N}$ für alle $r \in R$ gilt.

Bemerkung Wir beschäftigen uns von nun an nur noch mit einer ganzzahligen Norm auf einem Ring R. Das Attribut "ganzzahlig" wird aus diesem Grund stets fortgelassen.

Lemma 8 Sei R ein Ring, $\|\ \|_{\text{ind}}$ eine Norm auf R und $\mathfrak{a}$ ein Ideal von R. Dann ist $\|\ \|_{\text{ind}\,\mathfrak{a}}$ definiert durch

$$\|\bar{r}\|_{\text{ind}\,\mathfrak{a}} = \text{Min} \{\|x\|_{\text{ind}} \mid x \in \bar{r}\} \text{ für alle } \bar{r} \in R/\mathfrak{a}$$

eine Norm auf $\bar{R} = R/\mathfrak{a}$.

Beweis (AWØ), (AW1) und (AW3) sind trivialerweise erfüllt.

(AW4): $\|\bar{r}_1 \bar{r}_2\|_{\text{ind}\,\mathfrak{a}} = \|\overline{r_1 r_2}\|_{\text{ind}\,\mathfrak{a}} \leq \|xy\|_{\text{ind}} \leq k \|x\| \|y\|$

für alle $x \in \bar{r}_1$, $y \in \bar{r}_2$

Es folgt:

$$\|\bar{r}_1 \bar{r}_2\|_{\text{ind}\,\mathfrak{a}} \leq k \|\bar{r}_1\|_{\text{ind}\,\mathfrak{a}} \|\bar{r}_2\|_{\text{ind}\,\mathfrak{a}}$$

(AW2): Analog dem Beweis für (AW4).

Bemerkung a. Lemma 8 gilt für beliebige auch nicht-ganzzahlige Norm, wenn der Ring bezüglich der induzierten Metrik vollständig ist und $\mathfrak{a}$ abgeschlossen ist (Min ist durch inf zu ersetzen). Dann ist die Definition in Lemma 8 die in normierten Banach Algebren übliche.

b. Fordert man statt (AW1) nur (AW1'), so gilt in $R/\mathfrak{a}_o$ wieder (AW1). Die Abschwächung (AW1') ist aus diesem Grunde unwesentlich.

Definition 8 Ist R ein Ring mit der Norm $\|\ \|_{ind}$ und $\mathfrak{a}$ ein Ideal von R, so heisst die Norm $\|\ \|_{ind\,\mathfrak{a}}$ (gemäß Lemma 8) modulare Norm. Die durch $\|\ \|_{ind\,\mathfrak{a}}$ auf $R/\mathfrak{a}$ induzierte Metrik (wie in Lemma 7) modulare Metrik.

2.2 Fehlerkorrektur in Ringen mit einer Norm

Wir untersuchen von jetzt ab nur noch non-separate Codes und sprechen deshalb kurz von einem Code. Der Ring R sei mit einer Norm $\|\ \|_{ind}$ versehen, $K = R/\mathfrak{a}$ mit der modularen Norm $\|\ \|_{ind\,\mathfrak{a}}$. Dann sind R und $R/\mathfrak{a}$ nach Lemma 7 metrische Räume. Sind keine Missverständnisse zu befürchten, so schreiben wir die Norm $\|\ \|$, ohne alle Indizes.

Definition 9 Die minimale arithmetische Distanz D_{min} eines non-separaten Codes ist gleich dem minimalen Abstand der Punkte des Ideals $\mathfrak{y} \subset K = R/\mathfrak{a}$ bezüglich der modularen Metrik.

$$D_{min}\left[\ \|\ \|_{ind\,\mathfrak{a}}\ \mathfrak{y}\right] = \operatorname*{Min}_{\substack{x,\ y \in \mathfrak{y} \\ x \neq y}} \left\{\|x-y\|_{ind\,\mathfrak{a}}\right\}$$

Satz 9 Für einen non-separaten Code ist D_{min} gleich dem minimalen arithmetischen Gewicht W_{min}:

$$D_{min} = W_{min} = \operatorname*{Min}_{\substack{x \in \mathfrak{y} \\ x \neq 0}} \left\{\|x\|_{ind\,\mathfrak{a}}\right\}$$

Beweis Für $x, y \in \mathfrak{y}$ gilt

$$\|x - y\|_{ind\,\mathfrak{a}} = \|z\|_{ind\,\mathfrak{a}}$$

wo $z = x - y \in \mathfrak{J}$ ist. Umgekehrt gilt,

$$\| x - 0 \|_{\text{ind}\,\mathfrak{A}} = \| x \|_{\text{ind}\,\mathfrak{A}}$$

woraus schon die Behauptung folgt.

Satz 10 Ein non-separater Code kann alle Fehler aus

$$E_c(t) = \{x \mid x \in K,\ \| x \| \leq t\}$$

korrigieren und alle Fehler aus

$$E_d(t+s) = \{x \mid x \in K,\ t < \| x \| \leq t+s\}$$

erkennen, wenn gilt

$$D_{min} > 2t + s \quad (t, s \in \mathbb{N} \setminus \{0\})$$

Beweis Es ist klar, dass $(E_c \cup E_d) \cap \mathfrak{J} = E \cap \mathfrak{J} = \{0\}$ gilt. Nach Satz 3 brauchen wir nur noch zu zeigen, es existiert kein $e_1 \in E_c$ mit der Eigenschaft $\delta(e_1) = \delta(e_2)$ für ein $e_2 \in E \setminus \{0\}$. Aus $\delta(e_1) = \delta(e_2)$ folgt $e_1 - e_2 \in \mathfrak{J}$ und $\| e_1 - e_2 \| \leq \| e_1 \| + \| e_2 \| = 2t+s$, im Widerspruch zu $D_{min} > 2t + s$.

Corollar 10.1 Ein non-separater Code kann alle Fehler aus $E_d(d) = \{e \mid e \in K,\ \| e \| \leq d\}$ $(E_c = \{0\})$ erkennen, wenn gilt

$$D_{min} \geq d + 1 \quad (d > 0)$$

Corollar 10.2 Ein non-separater Code kann alle Fehler aus $E_c(t) = \{e \mid e \in K,\ \| e \| \leq t\}$ $(E_d = \{0\})$ korrigieren, wenn gilt

$$D_{min} \geq 2t + 1 \quad (t > 0)$$

Ist λ ein non-separater Code, so nennen wir die Elemente aus K Punkte und diejenigen aus $\mathfrak{J}$ Codepunkte. Die Sphäre vom Radius t um einen Punkt wird mit B (r, t) bezeichnet und ist durch

$$B(r,t) = \{x \mid x \in K,\ \| x - r \| \leq t\}$$

gegeben, $V_t = |B(r,t)|$ ist das Volumen der Sphäre. Da die Addition in K eine bezüglich der Norm stetige Operation ist, muss V_t unabhängig von r sein. Kann ein non-separater Code alle t-fachen Fehler korrigieren (d.h. $E_c(t) = \{e \mid e \in K,\ \| e \| \leq t\}$ und $E_d = \{0\}$), so gilt $B(r_1, t) \cap B(r_2, t) = \emptyset$ für alle $r_1, r_2 \in \mathfrak{J} (r_1 \neq r_2)$. Denn ist $r \neq 0$ ein Element aus dem Durchschnitt, dann gilt mit $e_1 = r - r_1$, $e_2 = r - r_2$, $e_1 \neq e_2$, $e_1, e_2 \in E_c$ und $e_1 - e_2 \in \mathfrak{J}$: e_1 und e_2 besitzen dasselbe Syndrom,

im Widerspruch zur Voraussetzung. Aus dieser Überlegung folgt die Ungleichung

$$|\mathcal{U}| \cdot V_t \leq |K|$$

Ist K endlich, so hat man $V_t \leq |R/\mathcal{U}|$.

Lemma 11 Ein non-separater Code, der alle t-fachen ($t > 0$) Fehler korrigiert, ist unter der Voraussetzung :K endlich, genau dann perfekt, wenn

$$V_t = |R/\mathcal{U}|$$

gilt.

Ist K nicht endlich, so muss gelten

$$K = \bigcup_{r \in \mathcal{U}} B(r, t)$$

Definition 10 Ein non-separater Code heisst bezüglich der Norm $\| \ \|$ äquidistant, wenn gilt.

$$\|x\| = \|y\| \quad \text{für alle } x, y \in \mathcal{U} \quad (x, y \neq 0)$$

Besitzen alle $x \in \mathcal{U}$ ($x \neq 0$) das gleiche Gewicht, bis auf genau einen Codepunkt, so wird der non-separate Code f(ast) - äquidistant genannt.

2.2.1 Rate und Redundanz

Um den zusätzlichen Aufwand und den Informationsverlust zu messen, ist es üblich, die Redundanz und die Rate eines non-separaten Codes als Masszahlen anzugeben.

Definition 11 Ist $\mathcal{M}$ endlich, so verstehen wir unter der Redundanz von λ die Zahl $Rd(\mathcal{M}) = \log|\mathcal{M}|$.

Unter der Coderate Rt verstehen wir die Zahl,

$$Rt(\mathcal{M}) = \frac{\log|\mathcal{U}|}{\log|K|}$$

vorausgesetzt $\mathcal{U}$ und K sind endlich.

Im Spezialfall $\lambda_g : \mathbb{Z}_m^+ \to \mathbb{Z}_{mg}^+$ gilt $Rd(m) = \log_q g$, wo q die Basis für das zur Darstellung gewählte Zahlensystem ist. Man setzt dann entsprechend

$$Rt(m) = \frac{\log_q m}{\log_q mg}$$

2.3. Eigenschaften der ganzzahligen Norm

Definition 12 Sei $\| \ \|$ eine k-Pseudobewertung auf dem Ring R. Wir definieren die folgenden Mengen:

$B(\| \ \|) = \{r \mid r \in R \text{ und } \|r\| \leq \|1\|\}$

$S(\| \ \|) = \{r \mid r \in R \text{ und } \|r\| = 1\}$

$P(\| \ \|) = \{q \mid q \in R \text{ und } \|qr\| = \|r\| \text{ für alle } r \in R\}$

Wir schreiben falls keine Missverständnisse zu befürchten sind, kurz B, S, P.

Lemma 12 Sei $\| \ \|$ eine k-Pseudobewertung auf R. Dann gilt:

(i) $P \subset S \subset B$, $0 \in B$, $\{1, -1\} \subset P$.

(ii) $-S = S$, $-P = P$, $-B = B$.

(iii) $q \in P \Rightarrow q$ ist Nichtnullteiler in R.

(iv) $P \cdot P = P$, $P \cdot S = S$

(v) $\|1\| = 1 \Rightarrow B = S \cup \{0\}$

$\|1\| = 1$ und $\| \ \|$ ist eine Pseudobewertung $\Rightarrow B \cdot B = B$ und $S \cdot S \subset S \cup \{0\}$

(vi) $q \in P \cap E(R) \Rightarrow q^{-1} \in P$ (E (R) ist die Einheitengruppe von R)

Definition 13 Sei $\| \ \|$ eine Norm auf R. Wir definieren:

(i) $E(P) = P \cap E(R)$

(ii) Gilt $\|1\| = 1$, so heisst die Norm unitär.

Lemma 13 E(P) ist eine (multiplikative) Untergruppe von E(R).

Definition 14 Auf der Menge aller k-Pseudobewertungen auf dem Ring R definieren wir die folgenden Relationen:

(i) $\| \ \|_1 \trianglelefteq \| \ \|_2 \Leftrightarrow B(\| \ \|_1) \subset B(\| \ \|_2)$, $S(\| \ \|_1) \subset S(\| \ \|_2)$ und $P(\| \ \|_1) \subset P(\| \ \|_2)$

(ii) $\| \ \|_1 \trianglelefteq \| \ \|_2$ und $\| \ \|_2 \trianglelefteq \| \ \|_1 \Longleftrightarrow \| \ \|_1 \simeq \| \ \|_2$ ($\| \ \|_1$ und $\| \ \|_2$ sind äquivalent)

Lemma 14 Die in der vorigen Definition eingeführte Relation " $\trianglelefteq$ " ist transitiv und reflexiv. Die Relation " $\simeq$ " ist eine Äquivalenzrelation.

Satz 15 Zu jeder Norm $\| \ \|$ auf einem Ring R für die gilt:

(AB) $B + B \subset B$

existiert eine unitäre Norm $\| \ \|_B \geq \| \ \|$.

Beweis Wir ändern die gegebene Norm $\| \ \|$ wie folgt ab:

$$\|r\|_B = \begin{cases} 1 + \left[\frac{\|r\|}{\|1\|}\right] & \text{falls } r \notin B \\ 1 & " \quad r \in B \text{ und } r \neq 0 \\ 0 & " \quad r = 0 \end{cases}$$

Wir müssen zeigen, dass $\| \ \|_B$ wieder eine Norm ist. Daß (AWØ), (AW1) und (AW3) erfüllt sind, ist sofort klar.

(AW2): $r_1, r_2 \in R$

a. $r_1 + r_2 \in B$ ($r_1, r_2 \neq 0$ da trivial, ebenso $r_1 + r_2 = 0$)

$1 = \|r_1 + r_2\|_B \leq \|r_1\|_B + \|r_2\|_B$

Denn $\|r_i\|_B = 1$ oder $\|r_i\|_B = 1 + \left[\frac{\|r_i\|}{\|1\|}\right] > 1 \quad (i = 1, 2)$.

b. $r_1 + r_2 \notin B$, d.h. $\|1\| < \|r_1 + r_2\| \leq \|r_1\| + \|r_2\|$

Wegen der Bedingung (AB) brauchen wir nur die Fälle $r_1, r_2 \notin B$ und $r_1 \in B$, $r_2 \notin B$ zu untersuchen.

$r_1, r_2 \notin B$: Folgt aus $[\alpha_1 + \alpha_2] \leq 1 + [\alpha_1] + [\alpha_2] \quad (\alpha_1, \alpha_2 \geq 0)$

$r_1 \in B$, $r_2 \notin B$: $\|r_1 + r_2\| \leq \|1\| + \|r_2\|$, woraus folgt

$\|r_1 + r_2\|_B \leq 1 + \|r_2\|_B = \|r_1\|_B + \|r_2\|_B$ (ausgenommen den trivialen Fall $r_1 = 0$)

(AW4): $r_1, r_2 \in R$

a. $r_1 \cdot r_2 \in B$ und $r_1 \cdot r_2 \neq 0$ ($r_1 \cdot r_2 = 0$ ist trivial)

Es gilt: $1 \leq \|r_1 \cdot r_2\| \leq \|1\|$ und $\|r_1 \cdot r_2\|_B = 1$

Sind $r_1, r_2 \in B$, so ist die Behauptung richtig, da $k \geq 1$ ist.

Die Fälle $r_1 \in B$, $r_2 \notin B$ sowie $r_1, r_2 \notin B$ sind ebenso einfach.

b. $r_1 \cdot r_2 \notin B$

Aus $r_1, r_2 \in B$ folgt $\|r_1 \cdot r_2\| \leq k \cdot \|1\|^2$, also

$\frac{\|r_1 \cdot r_2\|}{\|1\|} + 1 \leq k' + 1$ mit $k' = \left[k \cdot \|1\|\right] + 1$ Damit gilt

$\|r_1 \cdot r_2\|_B \leq (k' + 1) \cdot \|r_1\|_B \cdot \|r_2\|_B \quad (\|r_1\|_B = \|r_2\|_B = 1)$

Sei nun $r_1 \in B$, $r_2 \notin B$. Dann gilt $\|r_1\| \leq \|1\|$, also
$\|r_1 \cdot r_2\| \leq k \|1\| \|r_2\|$ und mit $k' = [k \cdot \|1\|] + 1$

$$\frac{\|r_1 \cdot r_2\|}{\|1\|} \leq k' \frac{\|r_2\|}{\|1\|} \text{. Weiter folgt:}$$

$$\|r_1 \cdot r_2\|_B - 1 \leq \left[k' \frac{\|r_2\|}{\|1\|}\right] \leq k'\left[\frac{\|r_2\|}{\|1\|}\right] + k' \leq (k' + 1)\left[\frac{\|r_2\|}{\|1\|}\right] + k'$$

d.h. $\|r_1 \cdot r_2\|_B \leq (k' + 1) \|r_1\|_B \cdot \|r_2\|_B$

Es gelte $r_1, r_2 \notin B$. Dann ergibt sich

$$\|r_1 \cdot r_2\| \leq k \|r_1\| \|r_2\| \text{ und } \frac{\|r_1 \cdot r_2\|}{\|1\|} \leq k' \frac{\|r_1\|}{\|1\|} \cdot \frac{\|r_2\|}{\|1\|}$$

mit k' wie oben definiert. Also

$$\|r_1 \cdot r_2\|_B \leq k' \frac{\|r_1\|}{\|1\|} \cdot \frac{\|r_2\|}{\|1\|} + 1 \leq k' \|r_1\|_B \cdot \|r_2\|_B + 1$$
$$\leq (k' + 1) \|r_1\|_B \cdot \|r_2\|_B$$

wegen $\|r_i\|_B \geq 1$ $(i = 1,2)$.

Da $k \leq k'$ gilt, ist $\|\ \|_B$ eine $(k' + 1)$-Pseudobewertung von R.
Es gilt $B(\|\ \|_B) = S(\|\ \|_B) \cup \{0\} = B(\|\ \|)$ und $P(\|\ \|) \subset P(\|\ \|_B)$ wie man leicht nachweist. Damit ist alles gezeigt.

Bemerkung

a. Statt der Bedingung (AB) kann man die folgende schwächere Forderung

$$(AB')\ r_1, r_2 \in B \Rightarrow \|r_1 + r_2\| < \|r_1\| + \|r_2\|$$

stellen (mit $r_1, r_2 \neq 0$). Für eine Pseudobewertung sind (AB) und (AB') äquivalent.

b. Auf der Menge aller k-Pseudobewertungen kann man noch eine Reihe weiterer Relationen definieren. So etwa die Relation $\leq_B$

$$\|\ \|_1 \leq_B \|\ \|_2 \iff B(\|\ \|_1) \subset B(\|\ \|_2)$$

und entsprechend definiert man die Relation $\approx_B$. Die Relation $\leq$ ist feiner als die Relation $\leq_B$. Satz 15 sagt dann aus, dass es zu jeder Norm $\|\ \|$, die (AB) bzw. (AB') genügt, eine B-äquivalente unitäre Norm $\|\ \|_B$ $(\|\ \| \approx_B \|\ \|_B)$ gibt. Es ist klar, wie man $\approx_S$ zu definieren hat.

Satz 16 Sei S ein erzeugendes System der abelschen Gruppe R^+, d h. jedes $r \in R$ lässt sich

$$r = \sum_{i \geq 1} \alpha_i s_i \qquad (s_i \in S,\ \alpha_i \in \mathbb{Z})$$

schreiben. Dann wird durch

$$\| r \|_S = \operatorname{Min} \left\{ \sum |\alpha_i| \,\middle|\, r = \sum \alpha_i s_i \right\}$$

eine k-Pseudobewertung definiert, wenn gilt $S \cdot S \subset k \cdot S$ mit $k \geq 1$.

Beweis (AWØ) - (AW3) weist man leicht nach. Sei nun $r_1 = \sum \alpha_i s_i$, $r_2 = \sum \beta_i s_i$ $(r_1, r_2 \in R)$ und $\| r_1 \|_S = \sum |\alpha_i|$, $\| r_2 \|_S = \sum |\beta_i|$. Es folgt,

$$r_1 \cdot r_2 = \sum_{i,j} (\alpha_i \cdot \beta_j)\, s_i \cdot s_j$$

wo $s_i, s_j \in k \cdot S$, gemäss der Voraussetzung $S \cdot S \subset k \cdot S$. Daraus ergibt sich

$$\| r_1 \cdot r_2 \|_S \leq k \cdot \sum_{i,j} |\alpha_i \beta_j| = k \cdot \sum_{i,j} |\alpha_i| \cdot |\beta_j| \leq k \| r_1 \|_S \| r_2 \|_S$$

Corollar 16.1 Gilt - $S \subset S$, so ist die Bedingung $S \cdot S \subset k \cdot S$ notwendig und hinreichend.

Beweis Wir können dann fordern $\alpha_i \geq 0$ in $r = \sum \alpha_i s_i$ und aus (AW4) folgt $\| s_1 \cdot s_2 \| \leq k \| s_1 \| \cdot \| s_2 \|$ für $s_1, s_2 \in S$. Wegen $\| s_1 \| = \| s_2 \| = 1$ gilt $\| s_1 \cdot s_2 \| \leq k$, d.h.

$$s_1 \cdot s_2 = \sum \gamma_i s_i \qquad (\gamma_i \geq 0)$$

wo $\sum \gamma_i \leq k$ ist, also $s_1 \cdot s_2 \in k \cdot S$ (den Index S haben wir fortgelassen).

Corollar 16.2 Die Norm $\| \ \|_S$ ist genau dann unitär, wenn $1 \in S$ oder $-1 \in S$ gilt, bzw. falls $-S \subset S$, genau dann wenn $1 \in S$ gilt.

Corollar 16.3 $S(\| \ \|_S) = S \cup -S$

Satz 17 Sei $\| \ \|$ eine Norm auf dem Ring R. Ist dann $S(\| \ \|)$ ein erzeugendes System für R^+, so ist $\| \ \|_S$ genau dann eine k-Pseudobewertung, wenn $S \cdot S \subset k \cdot S$ gilt. In diesem Fall hat man $S(\| \ \|_S) = S(\| \ \|)$, d.h. $\| \ \|_{\sim S} = \| \ \|_S$ und es gilt $\| r \| \leq \| r \|_S$ für alle $r \in R$.

Beweis Nach Lemma 12 (ii) gilt $S(\|\ \|) = -S(\|\ \|)$ und der erste Teil der Behauptung folgt aus Corollar 16.1. Aus $r = \sum \alpha_i s_i$ mit $s_i \in S, \alpha_i \geq 0$ folgt $\|r\| \leq \sum \|\alpha_i s_i\| \leq \sum |\alpha_i|$, also $\|r\| \leq \|r\|_S$. Die restlichen Behauptungen sind klar.

Bemerkung Wir setzen stets $\|0\|_S = 0$.

Beispiele Wir betrachten Ringe R mit zyklischer additiver Gruppe. Sei $a \in R$ ein erzeugendes Element von R^+. Setzen wir $S = \{a\}$, so können wir nach Satz 16 die Norm $\|\ \|_S$ einführen. Ist $r \in R$ mit $r = \alpha a$ $(\alpha \in \mathbb{Z})$ so gilt: $\|r\|_S = |\alpha|$. Insbesondere folgt für $R = \mathbb{Z}$ und $S = \{1\}$: $\|n\|_S = |n|$ $(n \in \mathbb{Z})$.
Fordern wir, dass R endlich ist, dann sind dies (siehe Peinado [48]) bis auf Isomorphie genau die Restklassenringe $\mathbb{Z}_m$. Setzen wir $S = \{\bar{1}\}$, so ist $\|\bar{n}\|_S = R_m(\bar{n})$ für alle $\bar{n} \in \mathbb{Z}_m$. Geht man dagegen von der Norm $\|\ \|_S$ auf $\mathbb{Z}$ aus und definiert $\|\ \|_S(m)$ wie in Lemma 8, so gilt $\|\bar{n}\|_{S(m)} = \text{Min}\{R_m(\bar{n}), m - R_m(\bar{n})\}$ für alle $\bar{n} \in \mathbb{Z}_m$.

Definition 15 Sei R ein algebraisches System und $(\Gamma, \cdot)$ eine Gruppe. Wir sagen Γ operiert auf R, wenn es eine (äussere) Komposition

$$\circ : \Gamma \times R \longrightarrow R$$

gibt mit den Eigenschaften:

(i) Die Abbildung $r \longrightarrow \gamma \circ r$ ist ein Automorphismus von R für jedes $\gamma \in \Gamma$ $(r \in R)$.

(ii) $(\varphi \cdot \gamma) \circ r = \varphi \circ (\gamma \circ r)$ für $\varphi, \gamma \in \Gamma$ und $r \in R$.

Wir sprechen auch von einer Darstellung von Γ auf R und schreiben (R, Γ).

Bemerkung

a. Eine Darstellung einer Gruppe Γ auf einem algebraischen System R ist äquivalent zu einem Homomorphismus

$$f : \Gamma \longrightarrow \text{Aut}(R)$$

Wo Aut (R) die Automorphismengruppe von R bezeichnet. Die Verknüpfung $\gamma \circ r$ schreiben wir von nun an γr.

b. In dieser Arbeit ist R stets ein Ring.

c. Wir setzen die Theorie der Paare (R,Γ) als bekannt voraus (siehe Plotkin [50] Chap. 2).

Definition 16 Sei R ein Ring mit der Norm $\|\ \|$. Dann bezeichnen wir mit $\Gamma_w(R)$ die Gruppe aller Bijektionen $\vartheta: R \to R$ mit der Eigenschaft

$$\|r\| = \|\vartheta(r)\| \quad \text{für alle } r \in R$$

Weiter setzen wir,

$$\Gamma_A(R) = \Gamma_w(R) \cap \mathrm{Aut}(R^+)$$

d.h. $\Gamma_A(R)$ besteht aus Automorphismen der additiven Gruppe von R.

Bemerkung Aus $\|r\| = 0 \iff r = 0$ folgt $\gamma(0) = 0$ für alle $\gamma \in \Gamma_w$.

Definition 17 Sei (R,Γ) ein Paar und $H \subset R$, $\Sigma \subset \Gamma$ Teilungen von R bzw. Γ.

(i) $C(H) = C_\Gamma(H) = \{\vartheta \mid \vartheta \in \Gamma \text{ und } \vartheta(h) = h \text{ für alle } h \in H\}$ (Γ-Zentralisator)

(ii) $N(H) = N_\Gamma(H) = \{\vartheta \mid \vartheta \in \Gamma \text{ und } \vartheta(H) = H\}$ (Γ-Normalisator)

(iii) $Z_R(\Sigma) = \{r \mid r \in R \text{ und } \vartheta(r) = r \text{ für alle } \vartheta \in \Sigma\}$ (Σ- Zentrum)

Lemma 18 $C(H)$ und $N(H)$ sind Untergruppen von Γ.

Lemma 19 Sei (R,Γ) ein Paar und R endlich. Dann gilt:

(i) $|\Gamma r| = \dfrac{|\Gamma|}{|C(r)|} = [\Gamma : C(r)]$

(ii) $|R| = \sum_{r \in \Omega} [\Gamma : C(r)]$

wo Ω ein Repräsentantensystem der verschiedenen Orbits Γr von R ist.

Satz 20 (Polya) Sei (R,Γ) treu und R endlich. Mit τ bezeichnen wir die Äquivalenzrelation, welche durch die Orbits von R definiert wird. Dann gilt:

$$|R/\tau| = \frac{1}{|\Gamma|} \cdot \sum_{\gamma \in \Gamma} |Z_R(\gamma)|$$

Satz 21 Sei $\lambda : \overline{R}^+ \to K^+$ ein non-separater Restklassencode, wo $K = R/m_\vartheta$ endlich ist. Dann ist $(\vartheta, N_{\Gamma_w}(\vartheta))$ ein Subpaar von

$(K,\Gamma_w(K))$, wo $\Gamma_w(K)$ in natürlicher Weise auf K operiert. Das Paar $(\mathfrak{g}, \overline{U})$ mit

$$\overline{U} = \{ f|\mathfrak{g}| \quad f \in N_{\Gamma_w}(\mathfrak{g})\}$$

ist treu. Aus

$$|\mathfrak{g} - 1| = [\overline{U} : C_{\overline{U}}(r)]$$

für ein $r \in \mathfrak{g} (r \neq 0)$ folgt λ ist äquidistant.

Beweis Aus Lemma 19 (i) folgt $|\overline{U}r| = |\mathfrak{g} - 1|$, d.h. es gibt nur zwei Orbits, den Nullorbit $\overline{U}0 = \{0\}$ und $\overline{U}r = \mathfrak{g}\setminus\{0\}$.
Nach Definition von $\overline{U}$ gilt $\|r_1\| = \|r_2\|$ für alle $r_1, r_2 \in \mathfrak{g}\setminus\{0\}$.

Lemma 22 Sei R ein Ring mit der Pseudobewertung $\| \ \|$ und $r \in E(R) \cap S(\| \ \|)$ eine Einheit von endlicher Ordnung. Dann gilt $r \in P(\| \ \|)$.

Beweis Sei $n \geq 1$ die Ordnung von r, dann folgt

$$\|1\| = \|r^n\| \leq \|r\|^n = 1 \quad \text{also } \|1\| = 1$$

sowie $r^i \in S(\| \ \|)$ für alle $i \geq 0$.

$$\|rx\| \leq \|r\| \ \|x\| = \|x\|$$

$$\|x\| = \|r \cdot r^{n-1} \cdot x\| \leq \|r^{n-1}\| \ \|rx\| = \|rx\|$$

d.h. $\|rx\| = \|x\|$ für alle $x \in R$.

Corollar 22.1 Sei R ein Ring mit einer Pseudobewertung $\| \ \|$ und $\mathfrak{a}$ ein Ideal in R. Gilt $r \in S(\| \ \|)$, $\overline{r} \in E(\overline{R})$ für ein $r \in R$ $(\overline{R} = R/\mathfrak{a})$ und ist $\overline{r}$ von endlicher Ordnung, so folgt $\overline{r} \in P(\| \ \|_{\mathfrak{a}})$.

Beweis Aus $\overline{r} \in E(\overline{R})$ folgt $r \notin \mathfrak{a}$, woraus man nach der Definition von $\| \ \|_{\mathfrak{a}}$ schon $\overline{r} \in S(\| \ \|_{\mathfrak{a}})$ schliesst. Alles weitere nach Lemma 22.

Bemerkung Lemma 22 und Corollar 22.1 gelten nur für Pseudobewertungen. Wir werden anschliessend ähnliche Aussagen für k-Pseudobewertungen ableiten ohne (AW4) zu benutzen.

Lemma 23 Sei R ein Ring mit der Norm $\| \ \|$ und $\mathfrak{a}$ ein Ideal in R. Gilt $r \in P(\| \ \|)$ für ein $r \in R$ und ist $\overline{r} \in E(\overline{R})$ von endlicher Ordnung, so hat man $\overline{r} \in P(\| \ \|_{\mathfrak{a}})$.

Beweis Sei $\| \overline{x} \|_{\mathfrak{a}} = \| y \| = \| ry \|$ für ein $y \in \overline{x}$ $(x, y, r \in R)$. Daraus folgt $\| \overline{r}\,\overline{x} \|_{\mathfrak{a}} = \| \overline{rx} \|_{\mathfrak{a}} \leq \| ry \| = \| \overline{x} \|_{\mathfrak{a}}$

also $\|\bar{r}\,\bar{x}\|_{\mathfrak{a}} \leq \|\bar{x}\|_{\mathfrak{a}}$. Es folgt ausserdem
$\|\bar{r}^i\,\bar{x}\|_{\mathfrak{a}} \leq \|\bar{r}\,\bar{x}\|_{\mathfrak{a}}$ für alle $i \geq 1$.

Ist n die Ordnung von $\bar{r}$, so
$\|\bar{x}\|_{\mathfrak{a}} = \|\bar{r}^n x\|_{\mathfrak{a}} \leq \|\bar{r}\,\bar{x}\|_{\mathfrak{a}} \leq \|\bar{x}\|_{\mathfrak{a}}$
und die Behauptung ist bewiesen.

Lemma 24 Voraussetzungen wie im vorigen Lemma und $\bar{r}^n = -\bar{1}$ für ein $n > o$. Dann gilt $\bar{r} \in P(\|\ \|_{\mathfrak{a}})$.
Beweis Wegen $\|-x\| = \|x\|$ $(x \in R)$ wie im vorigen Lemma.

Satz 25 Sei $\mathfrak{a}$ ein Ideal in R und (r), $\mathfrak{a}$ teilerfremd in R $((r) + \mathfrak{a} = R)$. Es gilt für $\mathfrak{a} \neq R$:
$\mathfrak{a}$, (r) teilerfremd $\Longleftrightarrow$ $\bar{r}$ ist Einheit in $\bar{R} = R/\mathfrak{a}$.

Lemma 26 Sei R ein Ring mit der Norm $\|\ \|$ und $T(P) \subset E(P)$ eine Untergruppe von $E(P)$. Dann operiert $T(P)$ treu auf R mittels
$(q \in T(P),\ r \in R)$ $q \circ r = T_q(r) = q \cdot r$ (Translation)
Es gilt $T(P) \subset \Gamma_A(R)$. Ist $\mathfrak{g}$ ein Ideal von R, so ist $N_{T(P)}(\mathfrak{g}) = T(P)$ und $\bar{T}(P) = \{T_q \mid \mathfrak{g} \mid \quad q \in T(P)\}$ operiert treu auf $\mathfrak{g}$.

Bemerkung Lemma 26 zusammen mit den Lemmata 22-24 legt ein praktisch brauchbares Verfahren nahe, um D_{min} für einen non-separaten Restklassencode $\lambda : \bar{R}^+ \longrightarrow K^+$ zu bestimmen. Dazu ist es nötig, ein $q \in P(\|\ \|)$ in den Ring R mit der Norm $\|\ \|$ zu finden mit der Eigenschaft $\bar{q} \in E(K)$. Falls $\bar{q}$ von endlicher Ordnung in $E(K)$ ist (z.B. K ist endlich), so gilt nach Lemma 23 $\bar{q} \in P(\|\ \|)$ $(\mathfrak{a} = m\mathfrak{g})$. Die von $\bar{q}$ erzeugte zyklische Gruppe $Z(\bar{q})$ ist Untergruppe von $\Gamma_A(K)$, $\bar{Z}(\bar{q})$ operiert treu auf $\mathfrak{g}$ wie aus Lemma 26 folgt. Jetzt sind wir in der Lage, die Orbitstruktur von $\bar{Z}(\bar{q})$ auf $\mathfrak{g}$ zu untersuchen, indem wir Lemma 19 und Satz 20 heranziehen. Gelingt es, ein Repräsentantensystem für die verschiedenen Orbits zu finden, so ist D_{min} bekannt (wir setzen $\mathfrak{g}$ als endlich voraus).

Satz 26 Sei $\lambda_g : Z_m^+ \longrightarrow Z_{mg}^+$ ein AN-Code und $\|\ \|$ eine Norm auf Z. Existiert ein $q \in P(\|\ \|)$ mit $(q, mg) = 1$, so gilt $\bar{q} \in E(P(\|\ \|_{(mg)}))$. Ist $\bar{Z}(\bar{q})$ wie in der letzten Bemerkung definiert,

so $[\overline{Z}(\overline{q}) : 1] = \omega_q(m)$ (Ordnung von q modulo m) und dies ist gerade die von q modulo m erzeugte zyklische Gruppe. Zu jedem Teiler d von m gibt es genau $\varphi(m/d) / \omega_q(m/d)$ Orbits von $\overline{Z}(\overline{q})$ auf $(\overline{g})$ mit $\omega_q(m/d)$ Elementen ($\omega_q(1) = 1$). Insgesamt gibt es

$$N = \sum_{d \mid m} \frac{\varphi(m/d)}{\omega_q(m/d)}$$

Orbits. Die vom Nullorbit $\overline{Z}(\overline{q}) \cdot 0 = \{0\}$ verschiedenen Orbits sind im wesentlichen durch die Nebenklassen von $Z(\overline{q})$ in $E(\mathbb{Z}_{m|d})$ gegeben.

Beweis Die erste Behauptung folgt aus Satz 25 und Lemma 23. Gilt $q^i gx \equiv q^j gx \bmod mg$ für $i, j \geq 0$ und alle $1 \leq x < m$, so ist dies äquivalent zu $q^i x \equiv q^j x \bmod m$, speziell für $x = 1$ $q^i \equiv q^j \bmod m$, woraus sich die Behauptung über die Struktur von $\overline{Z}(\overline{q})$ ergibt. Die restlichen Aussagen sind leicht einzusehen.

Corollar 26.1 Ist $q \in P(\| \|)$ und $mg = \sum_{i \geq 0} \alpha_i q^i$ ($\alpha_i \in \mathbb{Z}$) mit $(\alpha_0, q) = 1$, so gilt $\overline{q} \in E(P(\| \|_{(mg)}))$.

Corollar 26.2 Ist $m = p$ (p ungerade Primzahl) und q primitives Element modulo m mit $\overline{q} \in P(\| \|_{mg})$, so ist der AN-Code äquidistant.

Beweis Entweder direkt aus Satz 26 oder auch nach Satz 21.

Bemerkung Satz 26 ist das Fundament einer von Tsao-Wu [66] im Fall $mg = 2^l - 1$, $q = 2$ entwickelten Technik. Es zeigt sich, dass sie weitgehend verallgemeinert werden kann. Der Fall $mg = q^l - 1$ ist dadurch ausgezeichnet, dass sich wie wir später sehen werden, die Orbits einfach charakterisieren lassen. In diesem Zusammenhang wird auch Satz 26 noch einmal abgeleitet (vgl. Satz 79). Es ist klar, dass man basierend auf Satz 26 Algorithmen angeben kann, um D_{min} in einem konkreten Beispiel zu berechnen.
Die Transitivitätsgebiete einer Permutationshalbgruppe lassen sich nach J. Mc Kay und E. Regener (CACM 17, 8 (1974) 470, Algorithm 482) mit Hilfe einer ALGOL-Prozedur bestimmen.

Definition 18 Eine Folge $B = \{f_i\}_{i \geq 1}$ von positiven ganzen Zahlen heisst genau dann vollständig oder eine Basis, wenn sich jede positive ganze Zahl n in der Form

$$n = \sum_{i \geq 1} \alpha_i f_i \text{ mit } \alpha_i = \begin{cases} \emptyset \\ 1 \end{cases} \text{ für alle } i \geq 1$$

darstellen lässt.

Bemerkung Es ist $\alpha_i = 0$ für alle $i \geq N(n)$ und die Darstellung ist im allgemeinen nicht eindeutig.

Satz 27 Sei B eine Basis und $S = B \cup -B$. Jede ganze Zahl $n \in \mathbb{Z}$ lässt sich

$$n = \sum \alpha_i s_i \text{ mit } s_i \in S \text{ und } \alpha_i = \begin{cases} \emptyset \\ 1 \end{cases}$$

schreiben. Durch

$$\|n\|_S = \text{Min} \left\{ \sum \alpha_i \mid n = \sum \alpha_i s_i \right\}$$

wird genau dann eine k-Pseudobewertung definiert, wenn $S \cdot S \subset kS$ gilt ($k \geq 1$).

Beweis Vgl. Satz 16.

Satz 28 (Brown [7]) Sei $B = \{f_i\}_{i \geq 1}$ eine wachsende Folge positiver ganzer Zahlen mit $f_1 = 1$. B ist genau dann vollständig, wenn gilt $f_{k+1} \leq 1 + \sum_{i=1}^{k} f_i$ für $k = 1, 2, \ldots$.

Corollar 28.1 Ist B eine vollständige Folge, so gilt $f_i \leq \phi_i$, wo $\phi_i = 2^{i-1}$ ($i = 1, 2, \ldots$). Bezüglich der Sequenz $\{\phi_i\}$ ist die Darstellung $n = \sum \alpha_i \phi_i$ eindeutig und $\{\phi_i\}$ ist durch diese Eigenschaft charakterisiert.

Satz 29 Die Folge

(3) $1, 2, \ldots, q-1, 1 \cdot q, 2 \cdot q, \ldots, (q-1) \cdot q, 1 \cdot q^2, \ldots$

ist für jede natürliche Zahl $q \geq 2$ vollständig. Die Darstellung einer ganzen positiven Zahl ist nur für $q = 2$ eindeutig. Durch

$$\|n\|_q = \left\{ \text{Min} \sum \alpha_i \mid n = \sum \pm \alpha_i q^i \right\} \quad (n \in \mathbb{Z})$$

wird bei $q = 2$ eine Pseudobewertung und sonst eine 2-Pseudobewertung auf $\mathbb{Z}$ definiert.

Beweis Da jede natürliche Zahl eine (eindeutige) Darstellung

$$n = \sum_{i \geq 0} a_i q^i$$

mit $0 \leq a_i \leq q - 1$ besitzt, ist die Sequenz (3) vollständig. Für $q = 2$ ist diese Darstellung gerade die binäre Zahlendarstellung. Ist $q \geq 3$ so hat man $1 + 2 = 3$ und die Darstellung ist nicht eindeutig (was auch aus Corollar 28.1 folgt). Um zu zeigen, dass $\| \|_q$ eine Norm ist, genügt es nach Satz 27 $S \cdot S < k\,S$ nachzuweisen, was im Fall $q = 2$ trivial ist ($k = 1$). Bei $q \geq 3$ genügt es zu zeigen $aq^i \cdot bq^j \in S + S$ ($0 \leq a, b \leq q - 1$; $0 \leq i, j$) dies folgt aus $a \cdot b \leq (q-1)^2 < q^2$.

Bemerkung

a. Die in Satz 29 eingeführte Norm $\| \|_q$ wird in der Theorie der AN-Codes ausschliesslich benutzt. Wie wir noch sehen werden, ist diese Norm durch die Arbeitsweise der Addierer, welche man in Rechnern gemeinhin antrifft, notwendig bedingt.

b. Nach Satz 27 kann man jeder vollständigen Folge B, falls nur die Voraussetzung $S \cdot S \subset k\,S$ erfüllt ist, eine k-Pseudobewertung zuordnen. So ist z.B. die Folge der Fibonacci-Zahlen $F_1 = 1$, $F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$ ($n = 1,2, \ldots$) vollständig (siehe Brown [7]). Ob $S \cdot S \subset k\,S$ für ein $k \geq 1$ erfüllt ist, scheint offen zu sein, es muss $k > 1$ gelten ($F_3 \cdot F_4 \neq F_i$ für alle $i \geq 1$). Auch die Lucas-Sequenz $A_{n+2} = A_{n+1} + A_n$ ($A_1 = 2$, $A_2 = 1$; $n = 1,2, \ldots$), genauer die augmentierte Lucas-Sequenz, ist vollständig (siehe z.B. La Barbera [34]). Für diese Folge muss ebenfalls $k > 1$ gelten, sofern überhaupt $S \cdot S \subset k\,S$ erfüllt ist.

c. Setzt man $f_i = p_{i-1}$ mit $p_0 = 1$ und p_i ($i \geq 1$) die i-te Primzahl, so ist die Folge $\{f_i\}$ vollständig. Dies beweist man leicht durch Induktion nach i, da $p_{i+1} < 2p_i$ für alle $i \geq 1$ gilt (Bertrands Postulat).

d. Eine Theorie fehlerkorrigierender (non-separater) Codes lässt sich auch entwickeln, wenn man von einer Norm nur (AW0) - (AW3) verlangt Es könnte dann eine reizvolle, vielleicht sehr schwierige Aufgabe sein, D_{min} für die verschiedenen Ideale (g) bzw. $(\overline{g})$ in $\mathbb{Z}$ bzw. $\mathbb{Z}_m$ zu bestimmen, wenn man wie unter b angedeutet die Norm über Fibonacci- oder Lucas-Folge definiert. Der Rest dieser Arbeit beschäftigt sich damit, diese Aufgabe für die Norm $\| \|_q$ wenigstens partiell zu lösen.

e. Der Begriff der vollständigen Folge oder Basis lässt sich weitgehend verallgemeinern (siehe z. B. Brown [8], Long/Woo [37], de Bruijn [18] , etc.). Die Literatur über Fibonacci-Darstellungen und Ähnliches ist gerade in letzter Zeit stark angeschwollen, wie ein Durchblättern der letzten Jahrgänge des "Fibonacci Quarterly" zeigt

f. In der allgemeinen Theorie der (ganzzahligen) k-Pseudobewertungen lassen sich Untersuchungen noch über die Komposition von solchen Bewertungen durchführen. Hat man auf einem Ring R zwei Normen $\| \|_{ind1}, \| \|_{ind2}$, so ist z.B. $\| \|_{\Sigma} = \| \|_{ind1} + \| \|_{ind2}$ wieder eine Norm. Für Pseudobewertungen (im Sinne von Definition 6) liegt eine umfangreiche Arbeit von Cohn/Mahler [16] vor. Nicht ganz aussichtslos erscheinen Untersuchungen, bei denen man für bestimmte Klassen von endlichen Ringen die überhaupt möglichen Normfunktionen bestimmt. So ist z.B. die Struktur endlicher Ringe mit vorgegebener Einheitengruppe einigermassen bekannt. (vgl. J. Stewart: Finite Rings with a Specified Group of Units Math. Z. 126 (1972) 51 - 58).

g. Eine weitere Frage von vorerst nur mathematischem Interesse ist diejenige nach der Möglichkeit, k-Pseudobewertungen fortzusetzen auf Oberringe, etwa von R auf R [x] . Für Pseudobewertungen im Sinne von Mahler liegt eine Untersuchung von Nelson [46] vor, mit der Erweiterung auf Oberringe beschäftigt sich Huckaba [31] . Von mehr praktischem Interesse könnte vielleicht eine entsprechende Studie über die Fortsetzung von $\| \|$ auf Matrizenringe über R sein.

Kapitel 3

Fehler in der Integer-Arithmetik von Rechnern

Das Rechnen mit ganzen Zahlen, wie es in der Mathematik üblich ist, wollen wir als unbeschränkte Integer-Arithmetik bezeichnen; wir rechnen im Ring der ganzen Zahlen $\mathbb{Z}$. In einem Computer werden Zahlen zumeist binär verschlüsselt, eine unbeschränkte Integer-Arithmetik ist wegen der Endlichkeit solcher Maschinen nicht möglich. Man ist deshalb gezwungen, in dem endlichen Restklassenring $\mathbb{Z}_m$ zu rechnen. Häufig wird $m = 2^n$ oder $m = 2^n - 1$ gewählt. Die Funktion eines Addierers können wir uns in den verschiedenen Fällen durch die Graphen in Abb. 4 veranschaulichen. Die Knoten bezeichnen die elementaren Addierer, welche die Addition modulo zwei durchführen, die gerichteten Kanten zeigen den Fluss des carry-bits an.

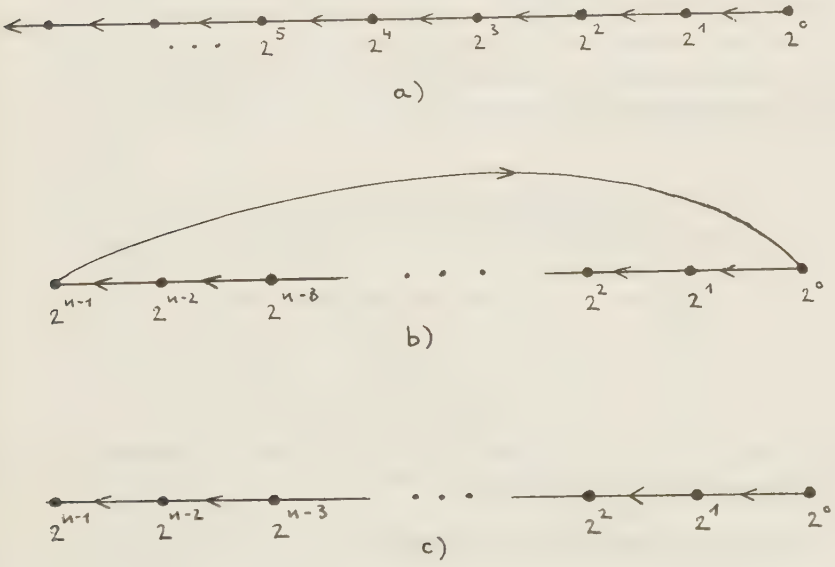


Abb. 4 Graphen, die den Fluss des carry-bits zeigen

a) unbeschränkte Integer-Addition
b) Addition modulo $2^n - 1$
c) Addition modulo 2^n

Ein Fehler kann durch inkorrekte modulo-zwei Summation eines elementaren Addierers entstehen oder durch Erzeugen eines falschen carry-bits. Tritt nur ein einziger solcher Fehler auf, so können wir von einem einfachen Fehler oder einem Fehler vom Gewicht eins sprechen. Bei einem Fehler vom Gewicht eins unterscheiden sich also korrekte und fehlerhafte Summe um $\pm 2^i$. Es liegt nun nahe, wenn sich korrekte und fehlerhafte Summe um die ganze Zahl e unterscheiden, das Gewicht von e zu definieren als die minimale Anzahl von Termen der Form $\pm 2^i$ welche für eine additive Zerlegung von e gebraucht werden. Ist diese Zahl etwa t, so bedeutet dies ja gerade, dass e nicht durch weniger als t einfache Fehler, die zusammen auftreten, entstanden sein kann. Es ist wichtig zu bemerken, dass diese Definition des Fehlergewichtes in den Fällen, die in Abb. 4 zu sehen sind, sinnvoll ist, nicht jedoch allgemein. Um das einzusehen, genügt es, den Graphen in Abb. 5 zu betrachten, der den carry-Fluss für eine modulo 9 Addition zeigt. Da

$$2 \cdot 2^3 = 16 \equiv 7 = 2^2 + 2^1 + 2^0 \bmod 9$$

gilt, folgt, dass jeder Fehler im carry-bit der Addiereinheit 2^3 zu einem dreifachen Fehler führt.

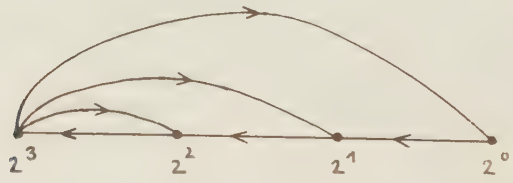


Abb. 5 Carry-Fluss bei der Addition modulo 9

Im nächsten Abschnitt werden wir die bisherigen Überlegungen verallgemeinern und exakt durchführen.

3.1 Normen auf dem Ring der ganzen Zahlen

Jede ganze Zahl n besitzt eine eindeutige (q-näre) Darstellung zur Basis q in der Form $n = \pm \sum_{i \geq 0} \alpha_i q^i$ $(q \geq 2)$ mit $0 \leq \alpha_i < q$.

Die Überlegungen im vorigen Abschnitt legen es nahe, Darstellungen der Form $n = \sum \alpha_i q^i$ mit $0 \leq |\alpha_i| < q$ zu untersuchen. Wir nennen sie modifizierte Darstellungen zur Basis q. Eine solche Darstellung ist nicht eindeutig (z. B. $3 = 4 - 1 = 2 + 1$, wenn $q = 2$).

Definition 19 Sei $n = \sum \alpha_i q^i$ eine modifizierte Darstellung der ganzen Zahl n zur Basis q und

$$w(n) = \sum_{i \geq 0} (1 - \delta(\alpha_i, \emptyset))$$

Für die q-näre Darstellung ist w(n) die Hamming-Norm und wird durch $\|n\|$ bezeichnet. Die (arithmetische) q-Norm $\|n\|_q$ von n ist dann die Zahl

$$\|n\|_q = \text{Min}\{w(n)\}$$

wobei das Minimum über alle modifizierten Darstellungen von n zur Basis q zu nehmen ist (vgl. Satz 29).
Wir suchen nun (bei gegebener Basis q) nach kanonischen Darstellungen für die ganzen Zahlen, bei denen die Anzahl der von Null verschiedenen Koeffizienten minimal ist. Eine solche kanonische Darstellung für beliebige Basis $q \geq 2$ wurde zuerst von Clark/Liang [14] angegeben, im Spezialfall $q = 2$ war schon früher von Reitwiesner [58] eine Darstellung, die NAF-Darstellung, gefunden worden.

Definition 20 Eine modifizierte Darstellung zur Basis q einer ganzen Zahl $n = \sum_{i \geq 0} \alpha_i q^i$ wird verallgemeinerte NAF-Darstellung (GNAF) genannt, wenn die folgenden beiden Bedingungen erfüllt sind:

(NA1) $|\alpha_i + \alpha_{i+1}| < q$ für alle i

(NA2) $\alpha_i \cdot \alpha_{i+1} < 0 \Rightarrow |\alpha_i| < |\alpha_{i+1}|$

Bemerkung

a. Für ein festes i folgt aus (NA2) die Bedingung (NA1). Ist α_i oder α_{i+1} gleich Null, so sind beide Bedingungen erfüllt. (NA1) muss also nur geprüft werden, wenn α_i und α_{i+1} ungleich Null sind.

b. Im Fall $q = 2$ erhält man die NAF-Darstellung. In diesem Fall sind (NA1) und (NA2) äquivalent zu

(NA) $\alpha_i \cdot \alpha_{i+1} = 0$ für alle i

c. Nimmt man wie in der Bemerkung b. nach Satz 29 angedeutet Fibonacci- oder Lucas-Zahlen zur Darstellung ganzer Zahlen, so existiert ebenfalls eine eindeutig bestimmte NAF-Darstellung (Zeckendorf's Theorem, vgl. Zeckendorf [69], Keller [32] oder Hoggat [29]). Ein Hinweis auf diesen Zusammenhang auch bei Preparata [51] p. 634 Bemerkung 4.

Beispiele

a. $q = 2$, $n = 7$
NAF : $1\emptyset\emptyset\bar{1}$ ("$\bar{1}$" steht für "-1")

b. $q = 3$
$n = 7$, GNAF: $1\emptyset\bar{2}$
$n = 309$, GNAF : $11\emptyset\bar{2}1\emptyset$

Eigenschaften der GNAF

Satz 30 (Minimalität) Ist n eine ganze Zahl, so ist die Norm $\|n\|_q$ gleich der Anzahl der von Null verschiedenen Koeffizienten in einer GNAF-Darstellung.
Beweis Siehe Clark/Liang [14]

Satz 31 (Eindeutigkeit) Sind

$$n = \sum \alpha_i q^i$$
$$n = \sum \beta_i q^i$$

zwei GNAF-Darstellungen der ganzen Zahl n, so gilt $\beta_i = \alpha_i$ für alle i.

Beweis Siehe Clark/Liang [14]

Satz 32 (Existenz) Sei $n = \sum \alpha_i q^i$ die q-näre Darstellung von n und $(q+1) \cdot n = \sum \gamma_i q^i$ ebenfalls die q-näre Darstellung. Dann ist

$$n = \sum \beta_i q^i$$

mit $\beta_i = \gamma_{i+1} - \alpha_{i+1}$ $(i \geq 0)$ die GNAF-Darstellung von n.

Beweis Siehe Clark/Liang [14]

Beispiel $q = 3$, $n = 309$

$$
\begin{array}{rl}
 & 1\emptyset211\emptyset\emptyset \quad 3\,n \\
+ & 1\emptyset211\emptyset \quad\;\; n \\
\hline
 & 12\emptyset\emptyset21\emptyset \quad 4\,n \\
- & 1\emptyset211\emptyset \quad\;\; n \\
\hline
 & 11\emptyset\overline{2}1\emptyset\emptyset \quad 3\,n \\
 & 11\emptyset\overline{2}1\emptyset \quad \text{GNAF}
\end{array}
$$

Dieser Satz beschreibt das zur Zeit einfachste Verfahren, um die GNAF-Darstellung und damit auch die Norm $\|n\|_q$ für eine ganze Zahl n von Hand zu berechnen. Es gibt noch eine Reihe anderer Algorithmen, die sich für die Berechnung durch einen Computer besser eignen.

3.2 Eigenschaften der Norm $\| \ \|_q$

Die Norm $\| \ \|_q$ ist unabhängig von der kanonischen GNAF-Darstellung auf $\mathbb{Z}$ definiert und es lassen sich auch viele ihrer Eigenschaften ableiten, ohne die GNAF-Darstellung zu benutzen. Die folgenden Eigenschaften ergeben sich unmittelbar aus Definition 19 (den Index q lassen wir fort).

Lemma 33 (i) $\|n\| = 0 \Longleftrightarrow n = 0$

(ii) $\|n+m\| \leq \|n\| + \|m\|$ $\quad (n, m \in \mathbb{Z})$

(iii) $\|n\| = \|-n\|$

(iv) $\|q^i n\| = \|n\|$ $\quad (i \geq 0)$

(v) $\|\alpha q^i\| = 1$ $(i \geq 0)$, $\alpha \in \{1,2,\ldots, q-1\}$

Lemma 34 $\|n-m\| \geq \big|\, \|n\| - \|m\| \,\big|$ $\quad (n, m \in \mathbb{Z})$

Lemma 35 (i) $\big|\, \|n\| - \|n \pm 1\| \,\big| = \begin{cases} \emptyset \\ 1 \end{cases}$

(ii) $q \nmid n \Longrightarrow \|n\| - \|n \pm 1\| = \begin{cases} \emptyset \\ 1 \end{cases}$

Lemma 36 Gilt $|n| \leq q^{k-1}$ $(n \in \mathbb{Z}, k \geq 1)$ und ist $n = \sum_{i \geq 0} \alpha_i q^i$ die GNAF-Darstellung von n, so ist $\alpha_i = 0$ für $i \geq k$ und $\alpha_{k-1} = \begin{cases} \emptyset \\ 1 \end{cases}$ falls $n \geq 0$, $\alpha_{k-1} = \begin{cases} \emptyset \\ -1 \end{cases}$ falls $n = 0$. Aus $|\alpha_{k-1}| = 1$ folgt $\alpha_{k-2} = 0$.

Beweis Für $k = 1$ ist das Lemma trivialerweise richtig. Es genügt den Fall $n \geq 0$, $n < q^{k-1}$ zu untersuchen. Es gilt $n = (\beta_{k-2}, \ldots, \beta_0)$ (q-näre Darstellung), daraus folgt $q \cdot n = (\beta_{k-2}, \ldots, \beta_0, 0)$ und $(q + 1)\, n = (\gamma_k, \gamma_{k-1}, \ldots, \gamma_0)$. Satz 32 gestattet dann die Folgerung $\alpha_i = 0$ für $i \geq k$ und $\alpha_{k-1} = \gamma_k = \begin{cases} \emptyset \\ 1 \end{cases}$. Aus $\alpha_{k-1} = 1$ folgt nach Definition der GNAF-Darstellung $\alpha_{k-2} \geq 0$. Nun folgt aber aus $\alpha_{k-2} > 0 : n \geq q^{k-1} + q^{k-2} - (q^{k-2} - 1) = q^{k-1} + 1$.

Corollar 36.1 Aus $q^{k-2} \leq |n| < q^{k-1}$ $(n \in \mathbb{Z},\ k > 1)$ und $\alpha_{k-1} = 0$ folgt $\alpha_{k-2} > 0$ falls $n > 0$ bzw. $\alpha_{k-2} < 0$ falls $n < 0$ gilt.

Satz 37 (i) $\|q^m \pm n\| = 1 + \|n\|$ falls $0 < n < q^{k-1}$ und $m \geq k+1$

(ii) $\|q^k + n\| = 1 + \|n\|$ falls $0 < n \leq q^{k-1}$

(iii) $\|q^k - n\| = \begin{cases} 1 + \|n\| \\ \|n\| \end{cases}$ falls $0 < n \leq q^{k-1}$ $(k \geq 1)$

Beweis Wir gehen aus von einer GNAF-Darstellung $(\alpha_{k-1}, \alpha_{k-2}, \ldots, \alpha_0)$ von n bzw. -n (Lemma 36)

(i): Folgt schon aus Definition 20.

(ii): Der Fall $\alpha_{k-1} = 0$ ist trivial. Für $\alpha_{k-1} = 1$, $q = 2$ folgt alles aus $2^k + 2^{k-1} = 2^{k+1} - 2^{k-1}$ und der Definition der NAF-Darstellung. Ist $q > 2$, so ist $(1, \alpha_{k-1}, \ldots, \alpha_0)$ schon die GNAF-Darstellung von $q^k + n$ und damit ist man fertig.

(iii): Der Fall $\alpha_{k-1} = 0$ ist trivial und für $q = 2$, $\alpha_{k-1} = -1$ folgt die Behauptung aus $2^k - 2^{k-1} = 2^{k-1}$ und der Definition der NAF-Darstellung. Der letzte Fall $q > 2$, $\alpha_{k-1} = -1$ ergibt sich aus $q^k - q^{k-1} = (q - 1)\, q^{k-1}$ und $\alpha_{k-2} = 0$.

Bemerkung

a. Ähnliche Aussagen wie in Lemma 36 und Satz 37 lassen sich auch für obere Schranken der Form αq^{k-1} mit $\alpha = 1, \ldots, q-1$ formulieren.

b. In den Beweisen von Lemma 36 und Satz 37 wird wesentlich die Existenz der GNAF-Darstellung benutzt. Es ist jedoch möglich, sämtliche Überlegungen durchzuführen und sich allein auf die Minimalität der Darstellung zu stützen. Wir wollen den Beweisgang kurz skizzieren. Sei $\alpha_l q^l$ der Summand mit maximalem Exponenten l und $\alpha_l \neq 0$ in einer minimalen modifizierten Darstellung von n (O.B.d.A. $n > 0$) und $n \leq q^{k-1}$. Ein solches l existiert, da die Anzahl der Glieder in einer minimalen Darstellung endlich ist (die q-näre Darstellung besteht schon aus endlich vielen Gliedern). Es kann nicht gelten $\alpha_l > 1$ und $l \geq k-1$, denn es würde folgen $n \geq \alpha_{k-1} q^{k-1} - (q^{k-1} - 1) > q^{k-1}$ ($\alpha_l < 0$ ist nicht möglich, da $n \leq -q^l + (q^l - 1) = -1$). Tritt in einer minimalen Darstellung ein Glied q^l auf, so muss gelten $\alpha_{l-1} \geq 0$, da sonst eine Verkürzung möglich ist. Aus $\alpha_{l-1} > 0$ folgt aber $n \geq q^l + q^{l-1} - (q^{l-1} - 1) = q^l + 1$. Damit ist gezeigt, dass falls $l \geq k-1$ ist, so muss notwendig $\alpha_l = 1$ und $\alpha_{l-1} > 0$ gelten. Daraus folgt $n \geq q^l - (q^{l-1} - 1) = (q-1) q^{l-1} + 1 > q^{l-1}$ und wegen $n \leq q^{k-1}$ ist $l \leq k-1$. Insgesamt ist durch diese Überlegungen Lemma 36 bewiesen. Ganz ähnliche Argumente gestatten dann den Beweis von Satz 37. Man erkennt, wie sich alle Beweise durch die Kenntnis der GNAF-Darstellung vereinfachen, während ohne sie eine detaillierte Analyse nötig ist.

Corollar 37.1 $\|q^k + n\| = \|q^k + m\| \iff \|n\| = \|m\|$ $(0 \leq n, m \leq q^{k-1})$

Corollar 37.2 Falls $0 \leq n \leq q^{k-1}$, so

$$\|q^k + q^{k-1} - n\| = \|(q^k + q^{k-1})(q-1) + n\|$$

Beweis
$$\begin{aligned}\|q^k + (q^{k-1} - n)\| &= 1 + \|q^{k-1} - n\| = \|q^{k+1} - (q^{k-1} - n)\| \\ &= \|(q^k + q^{k-1})(q-1) + n\|\end{aligned}$$

Lemma 38 $\|n \cdot m\|_q \leq (q-1)\|n\|_q \cdot \|m\|_q$ $(n, m \in \mathbb{Z})$

Beweis Sei $n = \sum_{i \geq 0} \alpha_i q^i$ eine minimale modifizierte Darstellung.

$$\begin{aligned}\|n \cdot m\|_q &= \|\sum (\alpha_i \cdot m) q^i\|_q \leq \sum \|\alpha_i m\|_q \\ &\leq \sum |\alpha_i| \, \|m\|_q \leq (q-1) \sum (1 - \delta(\alpha_i, 0)) \|m\|_q \\ &= (q-1) \|n\|_q \cdot \|m\|_q\end{aligned}$$

Bemerkung

a. $\|n\cdot m\|_q \leq \|n\|_q \cdot \|m\|_q$ gilt nur für $q = 2$. Ein einfaches Gegenbeispiel im Fall $q > 2$ ist $n = m = (q-1)\,q$, denn $\|(q-1)\,q\| = 1$ und $\|(q-1)^2\,q^2\| \leq \|(q-1)\,q\|\,\|(q-1)\,q\| = 1$. Wie man sofort einsieht, folgt aber aus $(q-1)^2 = (q-2)\,q + 1$, $\|(q-1)^2\,q^2\| = 2$.

b. Wie wir schon wissen, gilt nach Satz 29 sogar $\|n\cdot m\| \leq 2\|n\|\cdot\|m\|$.

Satz 39 Die durch Definition 19 eingeführte Norm $\|\ \|_q$ ist eine Pseudobewertung bei $q = 2$ und eine 2-Pseudobewertung für $q > 2$. Es gilt $q \in P(\|\ \|_q)$.

Beweis Sämtliche Behauptungen folgen direkt aus den bisher abgeleiteten Eigenschaften der Norm $\|\ \|_q$.

Satz 40 Gilt $|n| \geq q^{k-1}$ und $q^k > |n|$ $(n \in \mathbb{Z}, k \geq 1)$, so

(i) $\|n\|_2 \leq \left[\frac{k}{2}\right] + 1$

(ii) $\|n\|_q \leq k$

Beweis Nach Lemma 36 und der Definition der NAF-Darstellung.

Satz 41 $\|n\|_2 \leq |n| - \sum_{i\geq 1}\left[\frac{|n|}{2^i}\right]$ $(n \in \mathbb{Z})$

Beweis Im q-nären System gilt,

$$\sum_{i\geq 0}\alpha_i = |n| - (q-1)\sum_{i\geq 1}\left[\frac{|n|}{q^i}\right]$$

wenn $|n| = \sum_{i\geq 0}\alpha_i q^i$ die q-näre Darstellung ist. Daraus folgt für $q = 2$ der Satz.

Bemerkung

a. Um die Ungleichungen in Satz 40 und Satz 41 abzuleiten, ist es nicht nötig, auf die GNAF-Darstellung zurückzugreifen.

b. Wie das Beispiel $n = 11$ ($\|11\|_2 = 3$) zeigt, sind die oberen Schranken in Satz 40 (i) und in Satz 41 scharf. Die Abschätzung in Satz 41 ist jedoch besser, wie das Beispiel $n = 20$ ($\|20\|_2 = 2$) zeigt. Die obere Schranke in Satz 41 wird nämlich immer dann angenommen, wenn die binäre Darstellung schon die NAF-Darstellung ist.

c. Die Abschätzungen lassen sich in manchen Fällen noch etwas verbessern. Wie man sich leicht überlegt, verliert jeder Block der Form $\emptyset z_1 \ldots z_k \emptyset$ ($k \geq 3$), $z_i = q-1$ für alle $i = 1, \ldots, k$, bei der Umwandlung in die GNAF-Darstellung mindestens $k - 2$ Stellen ungleich Null; z.B. $n = 29$, $q = 2$: $\emptyset 111 \emptyset 1$, obere Schranke nach Satz 41 $\|29\|_2 \leq 4$ und der Block $\emptyset 111 \emptyset$ zeigt $\|29\|_2 \leq 3$ ($\|29\|_2 = 3$). Ein eventuelles "Überlappen" der Blöcke spielt dabei keine Rolle, ebensowenig eine fehlende Null bei einem "Kopf-" bzw. "Schwanzblock".

Satz 42 Sei $n \in \mathbb{Z}$ und $|n| = \sum_{i \geq 0} \alpha_i q^i$,

$$S_q(n) = \sum_{i \geq 0} (1 - \delta(\alpha_i, 0)) \, \delta(\alpha_{i+1}, 0)$$

d.h. $S_q(n)$ ist gleich der Anzahl von Blöcken $\emptyset z$ ($z = 1, 2, \ldots, q-1$) in der q-nären Darstellung von $|n|$. Dann gilt

$$S_q(n) \leq \|n\|_q$$

Beweis Dies folgt aus Satz 32 (Existenz der GNAF-Darstellung). $z = q-1$:

$$\begin{array}{lll} & *\emptyset\ q-1\ *\ * & q \cdot |n| \\ + & **\emptyset\ q-1\ * & |n| \\ \hline & **z_1\ z_2\ * & (q+1) \cdot |n| \quad z_1 = \begin{cases} \emptyset \\ q-1 \end{cases},\ z_2 = \emptyset, \ldots, q-1 \\ - & **\emptyset\ q-1\ * & |n| \\ \hline & *\,*z_1'\ z_2'\,* & \text{GNAF} \qquad z_1' = \begin{cases} \emptyset \\ q-1 \end{cases},\ z_2' = \overline{q-1}\ , \ldots, \emptyset \end{array}$$

Kritisch ist nur der Fall $z_1 = \emptyset$, $z_2 = q-1$, denn genau dann gilt $z_1' = z_2' = 0$. Dann haben wir notwendig:

$$\begin{array}{lll} & *\emptyset\ \ q-1\ \ q-1\,*\ \ q \cdot |n| & \\ + & *z\ \ \emptyset\ \ \ q-1\,* \qquad |n| & (z = 0, \ldots, q-1) \\ \hline & *z'\ \emptyset\ \ \ q-1\,* & (q+1) \cdot |n| \quad z' = \begin{cases} \emptyset \\ z+1 \end{cases} \\ - & *z\ \ \emptyset\ \ \ q-1\,* & |n| \\ \hline & *z''\ \emptyset\ \ \emptyset\ \ * & \text{GNAF} \end{array}$$

und $z'' \neq 0$. Ist $z \neq q-1$, so führt eine ähnliche (einfachere) Überlegung zum Ziel.

Lemma 43

$$s_2(n) = \sum_{i\geq 0} \left(\left(\left[\frac{|n|}{2^i} \right] - \left[\frac{|n|}{2^{i+2}} \right] \cdot 2^2 \right) \bmod 3 \right) \bmod 2$$

Bemerkung

a. Die Abschätzung nach Unten für $\|n\|_q$ in Satz 42 erfolgt nach einer von Mandelbaum [42] (im binären Fall) vorgeschlagenen Methode (die Verbesserung der Abschätzung nach Oben in Bemerkung c. nach Satz 41 findet sich in der gleichen Arbeit).

b. Die Abschätzung nach Satz 42 ist scharf, wie das Beispiel $q = 2$, $n = 21$ zeigt.

c. Ein Überlappen von Blöcken der Form $\emptyset z$ $(z \neq 0)$ ist nicht möglich. Bei Kopfblöcken kann natürlich die Null fehlen.

3.3 Fehlererkennung bei unbeschränkter Integerarithmetik

Sämtliche non-separaten Restklassencodes sind dann Abbildungen

$$\lambda_g : \mathbb{Z}^+ \to \mathbb{Z}^+$$

definiert durch

$$\lambda_g(n) = n \cdot g \quad (n \in \mathbb{Z})$$

Der für die Fehlerkorrektur grundlegende Satz 10 kann für die Norm $\|\|_q$ noch verschärft werden.

Satz 44 Damit ein non-separater Code bezüglich der Norm $\|\|_q$ alle Fehler aus $E_c(t)$ korrigieren und alle Fehler aus $E_d(t+s)$ erkennen kann, muss notwendig gelten $D_{min} > 2t + s$.

Beweis Aus $D_{min} \leq 2t + s$ würde folgen, es existieren zwei Codepunkte $ng \neq mg$ mit der Eigenschaft $\|ng - mg\|_q \leq 2t + s$. Ist $ng - mg = \sum_{i\geq 0} \alpha_i q^i$ die GNAF-Darstellung, so setzen wir

$e = \sum_{i>c} \alpha_i q^i$, $e' = \sum_{i=0}^{c} \alpha_i q^i$, so dass gilt $\sum_{i>c} (1 - \delta(\alpha_i, 0)) \leq t$ und $\sum_{i=0}^{c} (1 - \delta(\alpha_i, 0)) \leq t + s$. Ein solches c existiert stets und es gilt $e \neq 0$ oder $e' \neq 0$. Aus $\|e\|_q \leq t$ und $\|e'\|_q \leq t + s$ folgt $e \in E_c$, $e' \in E_d$, während $\delta(e-e') = 0$ ist, d.h. $\delta(e) = \delta(e')$ und es können nach Satz 3 nicht alle Fehler aus E_d entdeckt und alle Fehler aus E_c korrigiert werden.

Definition 21 Die Funktion $M_q : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \cup \{\infty\}$ ist definiert durch:

(i) $M_q(0, d) = M_q(g, 0) = M_q(g, 1) = 0$ für alle $g, d \in \mathbb{N}$

(ii) $M_q(g, d) = \text{Min}\{x \mid x \in \mathbb{N} \setminus \{0\} \text{ und } \|xg\| < d\}$ für alle $g, d \in \mathbb{N}$, $g \neq 0$, $d \neq 0, 1$ und falls diese Menge $\neq \phi$ ist.

(iii) $M_q(g, d) = \infty$ sonst.

Bemerkungen

a. d ist eine untere Schranke für D_{min} auf dem Intervall $[0, M_q(g, d))$ bzw. $(-\frac{1}{2} M_q(g,d), +\frac{1}{2} M_q(g,d))$ sofern $M_q(g, d) \neq 0$ gilt.

b. Statt $M_2(g, d)$ schreiben wir auch kurz $M(g, d)$.

Lemma 45 Es gilt:

(i) $M_q(q^i, d) = 1$ $(i \geq 0)$ und $d \neq 0,1$

(ii) $g \neq q^i$, 0 $(i \geq 0) \Longrightarrow M_q(g, 2) = \infty$

Definition 22 Sei $(q, g) = 1$, dann verstehen wir unter $L_q(g)$ die kleinste positive ganze Zahl mit der Eigenschaft:

$$q^{L_q(g)} \equiv \pm 1 \bmod g$$

Unter der Ordnung $\omega_q(g)$ von q modulo g verstehen wir die kleinste positive ganze Zahl mit $q^{\omega_q(g)} \equiv 1 \bmod g$.

Bemerkung Ist $q = 2$, so lassen wir den Index fort und schreiben $L(g)$, bzw. $\omega(g)$.

Durch den folgenden Satz wird die Gewichtsstruktur der AN-Codes auf $\mathbb{Z}$ vollständig beschrieben.

Satz 46 D_{min} kann in Abhängigkeit von g die folgenden Werte annehmen:

(i) $g = q^i$ $(i \geq 0) \Longrightarrow D_{min} = 1$

(ii) $(g, q) = 1 \Longrightarrow D_{min} = 2$

(iii) $(g, q) > 1 \Longrightarrow D_{min} \leq 2$

Beweis (i) klar!

(ii) Dies folgt aus $q^{\varphi(g)} \equiv 1 \bmod g$ oder $ng = q^{\varphi(g)} - 1$ für eine natürliche Zahl $n \geq 1$. Da $\varphi(g) > 1$ ist, hat man $\|ng\|_q = 2$.

(iii) Nach einem bekannten Satz der Zahlentheorie (siehe z.B. Vandiver/Weaver [67] p. 49, Theorem 8.2.3.) existieren dann ganze Zahlen b, $m \geq 1$ mit

$$q^{b+m} \equiv q^b \bmod g$$

oder $ng = q^{b+m} - q^b$, d.h. $\|ng\| \leq 2$.

Bemerkungen

a. Satz 46 bietet die Motivation für die Einführung von $M_q(g,d)$. Ohne weiter zu differenzieren, hat man nur triviale Ergebnisse.

b. Wegen Lemma 33 (iv) können wir O.B.d.A. $q \nmid g$ annehmen, was für $q = p$ (Primzahl) gerade $(g, q) = 1$ bedeutet.

Lemma 47 $2 \nmid g \Longrightarrow L(g) = \begin{cases} \omega(g) \\ \omega(g)/2 \end{cases} \quad (g > 1)$

Beweis Es genügt, anzunehmen $L(g) \neq \omega(g)$. Dann muss gelten $2^{L(g)} \equiv -1 \bmod g$, woraus $2^{2L(g)} \equiv 1 \bmod g$ folgt, d.h. $\omega(g) \mid 2\,L(g)$. Es gilt $L(g) \geq 2$, denn aus $L(g) = 1$ folgt $g = 3$ und die Behauptung ist richtig. Da $L(g)$ der grösste Teiler von $2\,L(g)$ ist, muss $\omega(g) \leq L(G)$ gelten, falls $\omega(g) \neq 2\,L(g)$. Aus der Annahme $L(g) \nmid \omega(g)$ folgt aber $L(g) \leq \omega(g)$, also $\omega(g) = L(g)$ und dies ist ein Widerspruch. Unter der Annahme $L(g) \nmid \omega(g)$ muss demnach $\omega(g) = 2\,L(g)$ gelten.

Corollar 47.1 $2 \nmid \omega(g) \Longrightarrow L(g) = \omega(g)$ und es existiert kein $i > 0$ mit $2^i \equiv -1 \bmod g$.

Corollar 47.2 $2 \mid \omega(g)$ und $g = p$ (Primzahl) $\Longrightarrow L(g) = \frac{\omega(g)}{2}$

Beweis $2^{\omega(g)} - 1 = (2^{\omega(g)/2} - 1)\,(2^{\omega(g)/2} + 1) \equiv 0 \bmod p$

Corollar 47.3 Sei $g = p$ Primzahl und 2 primitives Element modulo g, dann ist $L(g) = \frac{g-1}{2}$.

Corollar 47.4 $g = p$ und -2 primitives Element modulo g, dann gilt $L(g) = \frac{g-1}{2}$. Genau dann wenn $+2$ kein primitives Element ist gilt $2 \nmid L(g)$ und $\omega(g) = L(g)$.

Lemma 48 $(n, m) = 1$ und $2 \nmid n$, $m \Rightarrow \omega(n \cdot m) = k.g.V.\langle \omega(n), \omega(m) \rangle$

Satz 49 Sei $g = n \cdot m$, $2 \nmid g$ und $(n, m) = 1$, $(\omega(n), \omega(m)) = d$.
Dann gilt

$$L(g) = \begin{cases} \langle \omega(n), \omega(m) \rangle / 2 \text{ falls } 2 \mid d,\ 2 \nmid \frac{\omega(n)}{d},\ 2 \nmid \frac{\omega(m)}{d} \text{ sowie} \\ \qquad 2^{\frac{\omega(n)}{2}},\ 2^{\frac{\omega(m)}{2}} \equiv -1 \bmod n, m \\ \langle \omega(n), \omega(m) \rangle \quad \text{falls } 2 \mid d \text{ und } 2 \mid \frac{\omega(n)}{d} \text{ oder } 2 \mid \frac{\omega(m)}{d} \\ \langle \omega(n), \omega(m) \rangle \quad \text{falls } 2 \nmid d \end{cases}$$

Beweis Nach Lemma 48 $\omega(n \cdot m) = \langle \omega(n), \omega(m) \rangle$.

Fallunterscheidung:

a. $2 \nmid \omega(n)$ oder $2 \nmid \omega(m)$ (äquivalent zu $2 \nmid d$)
Ist $L(g) \neq \omega(n \cdot m)$, so $2^{L(g)} \equiv -1 \bmod g \Longrightarrow 2^{L(g)} \equiv -1 \bmod n$.
O.B.d.A. $2 \nmid \omega(n)$ und nach Corollar 47.1 führt dies zu einem Widerspruch.

b. $2 \mid d$

$$\omega(n) \cdot \omega(m) = \langle \omega(n), \omega(m) \rangle \cdot (\omega(n), \omega(m)) = d \cdot \langle \omega(n), \omega(m) \rangle$$

$$\omega(n \cdot m) = \frac{\omega(m)}{d} \cdot \omega(n) = k_1 \cdot \omega(n) = k_2 \cdot \omega(m)$$

Höchstens einer der k_i $(i = 1,2)$ kann gerade sein, der andere Faktor muss dann ungerade sein.

b1) $2 \mid \frac{\omega(n)}{d}$ oder $2 \mid \frac{\omega(m)}{d}$

Sei k_1 gerade. Gilt $L(g) = \omega(n \cdot m)$ so sind wir fertig.
Aus $L(g) \neq \omega(n \cdot m)$ folgt nach Lemma 47 $L(g) = \frac{\omega(n \cdot m)}{2}$
und $2^{k_1 \omega(n)/2} = 2^{\omega(n \cdot m)/2} \equiv -1 \bmod n \cdot m$
impliziert $2^{k_1 \omega(n)/2} \equiv -1 \bmod n$, im Widerspruch zu $2^{\frac{k_1}{2}\omega(n)} \equiv 1 \bmod n$

b2) $2 \nmid \frac{\omega(n)}{d}$ und $2 \nmid \frac{\omega(m)}{d}$ und $2^{\omega(n)/2}, 2^{\omega(m)/2} \equiv -1 \bmod n, m$

Sind n und m Primzahlen, so folgt aus

$2^{\omega(n)} - 1 = (2^{\omega(n)/2} - 1)(2^{\omega(n)/2} + 1) \equiv 0 \bmod n$ schon

$2^{\omega(n)/2} \equiv -1 \bmod n$ bzw. $2^{\omega(m)/2} \equiv -1 \bmod m$. Aus $2 \nmid k_1$

und $2 \nmid k_2$ folgt

$$2^{\langle \omega(n),\, \omega(m) \rangle/2} = (2^{\omega(n)/2})^{k_1} \equiv -1 \bmod n$$

$$2^{\langle \omega(n),\, \omega(m) \rangle/2} = (2^{\omega(m)/2})^{k_2} \equiv -1 \bmod m$$

Wegen $(n, m) = 1$ gilt dann

$$2^{\langle \omega(n),\, \omega(m) \rangle/2} \equiv -1 \bmod n \cdot m$$

Was zu zeigen war.

Corollar 49.1 Für $g = p_1 \cdot p_2$, wo p_1, p_2 ungerade Primzahlen sind, ist die Fallunterscheidung in Satz 49 vollständig, d.h. es gilt

$$L(g) = \begin{cases} \langle \omega(p_1), \omega(p_2) \rangle/2 & \text{falls } 2 \mid d \text{ und } 2 \nmid \frac{\omega(p_1)}{2},\ 2 \nmid \frac{\omega(p_2)}{2} \\ \langle \omega(p_1), \omega(p_2) \rangle & \text{sonst} \end{cases}$$

Bemerkung Durch $g = \prod p_i^{\alpha_i}$ hat man eine Zerlegung in paarweise Teilfremde Faktoren. Eine entsprechende Modifikation von Satz 49 gestattet es in vielen Fällen $L(g)$ zu berechnen.

Lemma 50 Ist $q > 1$ eine natürliche Zahl, so gilt

(i) $q^m - 1 \mid q^n - 1 \iff m \mid n$

(ii) $q^m + 1 \mid q^n - 1 \iff (m \mid n \text{ und } 2 \mid \frac{n}{m})$

(iii) $q^m + 1 \mid q^n + 1 \iff m \mid n \text{ und } 2 \nmid \frac{n}{m}$

für alle natürlichen Zahlen $m, n > 0$.

Beweis (i) $\Longrightarrow$: $q^m - 1 \mid q^n - 1 \Longrightarrow q^n - 1 \equiv 0 \bmod (q^m - 1)$

Es gilt $n = a \cdot m + r$ $(a \geq 0,\ 0 < r < m)$, woraus folgt

$q^n - 1 \equiv q^r - 1 \equiv 0 \bmod (q^m - 1)$ (wegen $q^m \equiv 1 \bmod (q^m - 1)$).

Da $r > 0$ nicht gelten kann, folgt $r = 0$.

$\Longleftarrow$: Gilt $m \mid n$, so ist

$$(q^m - 1)(q^{n-m} + q^{n-2m} + \ldots + 1) = q^n - 1$$

(ii) $\Longrightarrow$: $q^m + 1 \mid q^n - 1 \Longrightarrow q^n \equiv 1 \bmod (q^m + 1)$. Aus $m \mid n$ folgt wegen $q^m \equiv -1 \bmod (q^m + 1)$, $(q^m)^a \equiv (-1)^a \equiv 1 \bmod (q^m + 1)$, wobei $n = a \cdot m$, d.h. $2 \mid a$. Dass $m \mid n$ gilt, zeigt man wie unter (i)

$\Longleftarrow$: Gilt $m \mid n$ und $2 \mid \frac{n}{m}$, so

$$(q^m + 1)\,(q^{n-m} - q^{n-2m} \pm \ldots - 1) = q^n - 1$$

(iii) Wie unter (i) oder (ii).

Definition 23 Sei $M > 1$ eine natürliche Zahl.

$$D_{min}\,[0, M)_q = \text{Min}\,\{\|gx\|_q \mid x \in (0, M)\}$$

Statt $D_{min}\,[0, M)_2$ schreiben wir $D_{min}\,[0, M)$.

3.3.1 Berechnung von M_2 (g, d)

Mit Lemma 45 sind die Werte der Funktion M_2 (g,d) für alle Argumente $d = 0,1,2$ und $g \in \mathbb{N}$ bekannt. Als erste Aufgabe stellt sich die Frage nach dem Wert von M_2 (g, 3).

Lemma 51 (Peterson [49])

$(M > 1)$ $D_{min}\,[0, M) \geq 3 \Longleftrightarrow (2^i \equiv g\,(M-1) + 1 \Longrightarrow \pm 2^i \not\equiv 0 \bmod g$ und $\pm 2^i \not\equiv \pm 2^j \bmod g$ für $i \neq j)$

Beweis

$\Longleftarrow$: Keine der Zahlen xg, $x \in [0, M)$ kann für ein $x \neq 0$ vom Gewicht 0 oder 1 sein. Angenommen $xg = \pm 2^i \pm 2^j$ mit $i > j + 1$ $j \geq 0$ sei die NAF-Darstellung. Da $xg > 0$ folgt, $xg = + 2^i \pm 2^j$. Wir unterscheiden die Fälle:

a. $xg = + 2^i + 2^j \Longrightarrow 2^i \equiv - 2^j \bmod g$ und $2^i,\ 2^j < g\,(M - 1)$

b. $xg = + 2^i - 2^j = 2^j\,(2^{i-j} - 1)$

Es genügt, den Fall $xg = 2^i - 1$ für $i > 1$ und $(g, 2) = 1$ zu betrachten. Ist $0 < x < M-1$, so folgt $2^i,\ 2^0 < g\,(M-1)$ und $2^i \equiv 2^0 \bmod g$.

Gilt $g\,(M-1) = 2^i - 1$, so hat man $2^i,\ 2^0 < g\,(M-1) + 1$ und ebenfalls $2^i \equiv 2^0 \bmod g$.

$\Longrightarrow$: Diese Richtung ist trivial.

Satz 52 Sei $g > 1$, $2 \nmid g$. Dann gilt:

$$M_2(g, 3) = \begin{cases} \frac{2^{L(g)} - 1}{g} & \text{falls } 2^{L(g)} \equiv 1 \bmod g \\ \frac{2^{L(g)} + 1}{g} & \text{falls } 2^{L(g)} \equiv -1 \bmod g \end{cases}$$

Beweis Es kann nicht $2^{L(g)} \equiv 1$ und $2^{L(g)} \equiv -1 \bmod g$ gelten, denn daraus würde $2 \equiv 0 \bmod g$ folgen. Sei $2^{L(g)} \equiv 1 \bmod g$, dann hat man:

$$2^{L(g)} \equiv 1 \bmod g \iff 2^{L(g)} - 1 = x_1 g \quad (x_1 \neq 0)$$

$$\iff \quad M_2(g,3) \leq x_1 = \frac{2^{L(g)} - 1}{g}$$

Weiter gilt

$(x \neq 0)$ $\|xg\|_2 \leq 2 \iff \|xg\| = 2$ (nach Satz 46 (ii))

$\iff xg = 2^j \pm 2^i \quad (j > i \geq 0)$

$\iff 2^i (2^{j-i} \pm 1) \equiv 0 \bmod g$

$\iff 2^{j-i} \pm 1 \equiv 0 \bmod g$

$\iff j - i \geq L(g)$

$\iff xg = 2^i (2^{j-i} \pm 1) \geq 2^{L(g)} - 1 = x_1 g$

$\iff x \geq x_1$

Analog schliesst man im Fall $2^{L(g)} \equiv -1 \bmod g$.

Bemerkung Satz 52 wurde von Brown [6] 1960 in einer Arbeit veröffentlicht, der eine kurze Mitteilung von Diamond [19] aus dem Jahre 1955 zugrunde liegt. In der Note von Diamond werden die AN + B-Codes eingeführt.

Lemma 53 (Peterson) Sei $g > 1$, dann gilt

$M_2(g, 3) = m > 1 \iff (2^i < g \ (M-1) \Rightarrow \pm 2^i \not\equiv 0 \bmod g$ und

$\pm 2^i \not\equiv 2^j \bmod g$ für $i \neq j$) und $\|gm\| \leq 2$

Beweis Der Beweis läuft ebenso wie in Lemma 51, bis auf Fall b. Gilt $g(m-1) = 2^i - 2^0$, so folgt $2 \mid m$, d.h. $3 \leq \|g \frac{m}{2}\| = \|gm\| \leq 2$, Widerspruch!

Satz 54 (Peterson [49]) Ist $g > 1$ eine ungerade Primzahl und entweder 2 oder - 2 primitives Element modulo g, so gilt

$$M_2(g, 3) = \begin{cases} \frac{2^\tau - 1}{g} & \text{falls - 2 primitives Element ist, aber } \underline{\text{nicht}} \text{ + 2} \\ \frac{2^\tau + 1}{g} & \text{falls + 2 primitives Element ist} \end{cases}$$

mit $\tau = \frac{g-1}{2}$

Beweis Sei - 2 primitives Element modulo g aber nicht + 2. Aus Corollar 47.4 folgt $L(g) = \frac{g-1}{2}$ und $2^{L(g)} \equiv 1 \bmod g$. Aus Satz 52 ergibt sich die Behauptung. Entsprechend einfach ist der Beweis für die alternative Behauptung.

Bemerkung In Satz 54 gilt auch die Umkehrung, ist eine der Beziehungen richtig, so ist g Primzahl und 2 bzw. - 2 primitives Element.

Satz 55 Es gilt:
(i) Sei $g \cdot M(g,d) = 2^n - 1$. Ist m ein echter Teiler von n mit der Eigenschaft $(g, 2^m - 1) = 1$ oder $(g, 2^m + 1) = 1, 2 \mid \frac{n}{m}$, so gilt

$$D_{min}[0, M(g,d)) \leq \frac{n}{m}$$

(ii) Sei $g \cdot M(g,d) = 2^n + 1$. Ist $m \neq n$ ein Teiler von n mit der Eigenschaft $(g, 2^m + 1) = 1$ und $2 \nmid \frac{n}{m}$, so gilt

$$D_{min}[0, M(g,d)) \leq \frac{n}{m}$$

Beweis (i) Nach Lemma 50 kann man schreiben $(n > 0)$

$$2^n - 1 = (2^m - 1)(2^{n-m} + \ldots + 1)$$

bzw. $$2^n - 1 = (2^m + 1)(2^{n-m} - 2^{n-2m} \pm \ldots - 1)$$

Da nach Voraussetzung $(g, 2^m \pm 1) = 1$, so ist $(2^{n-m} + \ldots + 1)$ oder $(2^{n-m} \mp \ldots - 1)$ ein Codepunkt aus dem Intervall $[0, M(g,d))$, dessen Gewicht höchstens gleich $\frac{n}{m}$ sein kann. Wie man sich leicht überlegt, ist der Fall n = 0 trivial.
(ii) Entsprechend wie unter (i).

Corollar 55.1 Es gilt:

(i) $g\,M(g, 3) = 2^{L(g)} - 1$ wie in Satz 55 ($M(g,d) > 1$). Ist dann A der grösste unter den echten Teilern m von $L(g)$ mit $(g, 2^m - 1) = 1$ oder $(g, 2^m + 1) = 1$, $2 \nmid \frac{L(g)}{m}$, dann gilt

$$3 \leq D_{min} \leq \frac{L(g)}{A}$$

(ii) $g\,M(g, 3) = 2^{L(g)} + 1$ ($M(g, 3) > 1$). Ist A der grösste unter den Teilern $m \neq L(g)$ von $L(g)$ mit $(g, 2^m + 1) = 1$ und $2 \nmid \frac{L(g)}{m}$, so gilt

$$3 \leq D_{min} \leq \frac{L(g)}{A}$$

(iii) Ist g eine Primzahl und entweder + 2 oder - 2 primitive Wurzel, so $L(g) = \frac{g-1}{2}$ und $(g, 2^m \pm 1) = 1$ ist stets erfüllt. Man erhält, bei entsprechend schwächeren Voraussetzungen, dieselben Resultate wie unter (i) bzw. (ii).

Bemerkung

a. In Satz 55 benutzen wir eine von Hartman/Tzeng [28] angegebene Technik.

b. Es lassen sich durch "geschickte" Wahl von g AN-Codes finden für die sich $M(g, d)$ bei einem bestimmten d angeben lässt. Wählt man z.B. $g = (2^n - 1) / (2^{n_1} - 1)(2^{n_2} - 1)$ mit $(n_1, n_2) = 1$, $n_2 > n_1 \geq 2$ und $n = n_1 n_2$, so gilt nach Chen/Chen/Liu [9],

$$M(g, n_1) = (2^{n_1} - 1)(2^{n_2} - 1)$$

Für weitere, ähnliche Ergebnisse siehe Rao [54].

3.3.2 Berechnung von $M_q(g, d)$ für $q \geq 2$

Lemma 56 Aus $(g, q) = 1$, $g \mid q^n - 1$ ($n \geq 1$), $g > q$ und $\alpha q^i \not\equiv \beta \bmod g$ für alle $i = 0, \ldots, n-1$ und $0 < |\alpha|, |\beta| < q$, (O.B.d.A $0 < \alpha, |\beta| < q$)

(ausgenommen $i = 0, \alpha = \beta$) folgt

$$g \cdot M_q(g, 3) = q^n - 1$$

Beweis Klar ist $M_q(g, 3) = q^n - 1/g$. Aus $g > q$ und $(g,q) = 1$ folgt, dass niemals $gx = \alpha q^i$ für ein $x \geq 1$, $i \geq 0$ gelten kann. Wäre $M_q(g, 3) < q^n - 1/g$, so würde ein $1 \leq x' < q^n - 1/g$ existieren mit

$$gx' = \alpha' g^k + \beta' q^l \quad (k, l \geq 0;\ 0 < |\alpha'|, |\beta'| < q)$$

Was äquivalent ist zu

$$gx = \alpha q^i - \beta \quad (0 < |\alpha|, |\beta| < q)$$

d.h. $\alpha q^i \equiv \beta \bmod g$. Dass $0 \leq i \leq n - 1$ gelten muss, überlegt man sich leicht.

Satz 57 Sei $g = (q-1)\, p^n$ $(n \geq 1)$, $p > q$ (p Primzahl) und es gelte

(NR) $(x - q + 1)\, x^{-1} \notin Z_p(q)$ (die von q modulo p erzeugte zyklische Gruppe)

für alle $0 < x < q-1$ $(xx^{-1} \equiv 1 \bmod p)$.

Dann ist

$$g \circ M_q(g, 3) = q^\lambda - 1$$

mit $\lambda = \omega_q(p^n)$, falls $-1 \notin Z_p(q)$.

Beweis Aus den Voraussetzungen folgt $g \mid q^\lambda - 1$, $g > q$ und $(g,q) = 1$. Es genügt also wegen Lemma 56 die Annahme $\alpha q^i \equiv \beta \bmod g$ $(i = 0, \ldots, \lambda-1;\ 0 < |\alpha|, |\beta| < q)$ zum Widerspruch zu führen. Aus einer solchen Annahme folgt

(4) $\alpha q^i \equiv \beta \bmod p^n$

(5) $\alpha q^i \equiv \beta \bmod q-1$

weil $(p, q-1) = 1$ ist. Aus (5) ergibt sich, da $q^i \equiv 1 \bmod q-1$ ist $\alpha \equiv \beta \bmod q-1$. Haben α und β gleiches Vorzeichen, so müssen sie gleich sein, Widerspruch zu (4)! Die eine Möglichkeit, welche noch bleibt, ist $\alpha = \beta + (q-1)$ $(0 < \alpha < q-1, \beta < 0$ O.B.d.A.), $\alpha \neq \beta$. Wegen (4) a fortiori $\alpha q^i \equiv \beta \bmod p$, einsetzen der letzten Gleichung liefert $\alpha q^i \equiv \alpha - (q-1) \bmod p$, also $q^i \equiv (\alpha - q+1)\alpha^{-1} \bmod p$ im Widerspruch zu (NR). Damit verbleibt als einziger Fall noch $\alpha = q-1$ und $\beta = -(q-1)$, was nach Bedingung (4) auf $q^i + 1 \equiv 0 \bmod p$ führt, d.h. $-1 \in Z_p(q)$ im Widerspruch zur Voraussetzung.

Corollar 57.1 (Neumann/Rao [47]) Voraussetzungen wie im vorigen Satz und n = 1. Dann sind - $1 \notin Z_p$ (q) und Bedingung (NR) notwendig und hinreichend für

$$g \cdot M_q\ (g,\ 3) = q^{\lambda} - 1$$

Corollar 57.2 Sei -q aber nicht q primitives Element modulo p (p Primzahl) und die Voraussetzungen wie in Satz 57. Dann ist die Bedingung (NR) hinreichend für

$$g \cdot M_q\ (g,\ 3) = q^{\lambda} - 1$$

mit $\lambda = \omega_q(p^n) = \frac{p-1}{2} \cdot p^t$, $t = \text{Max}\ \{0,\ n-z\}$ wo $p^z \parallel (q^{\frac{p-1}{2}} - 1)$.

Beweis Da q nicht primitives Element modulo p ist, muss gelten - $1 \notin Z_p$ (q). Alles weitere folgt aus Satz 57 und mit Hilfe von ein wenig elementarer Zahlentheorie.

Corollar 57.3 (Neumann/Rao [47]) Sei $g = (q-1)\ p$ und die Voraussetzungen wie im vorigen Corollar. Dann ist (NR) notwendig und hinreichend für

$$g \cdot M_q\ (g,\ 3) = q^{\frac{p-1}{2}} - 1$$

Satz 58 Sei $g = (q^2 - 1)\ p^n$ $(n \geq 1)$, $p > q + 1$, $2 \mid q$ (p Primzahl) und sonst dieselben Voraussetzungen wie in Satz 57 sowie $2 \mid \lambda$. Dann gilt

$$g \cdot M_q\ (g,\ 3) = q^{\lambda} - 1$$

Beweis Es genügt zu bemerken, dass $q^2 - 1 = (q + 1)\ (q - 1)$ ist und aus den Voraussetzungen $(q + 1,\ p) = (q - 1,\ p) = (q+1, q-1) = 1$ folgt, sowie $2 \mid \lambda$ schon $q + 1 \mid q^{\lambda} - 1$ impliziert. Alles Weitere wie im Beweis zu Satz 57.

Bemerkung

a. Satz 57 verallgemeinert ein Resultat von Neumann/Rao [47] (vgl. auch Rao [54]). Setzt man in Corollar 57.3 q = 2, n = 1, so ergibt sich Satz 54 teilweise als Spezialfall, ebenso für q = 3 Ergebnisse von Rao/Trehan [52]. In dem von Neumann/Rao [47] gegebenen Beweis für Corollar 57.3 ist eine Lücke enthalten.

Es dürfte klar sein, dass sich auch aus Satz 58 einige Corollare ableiten lassen. Auch der Satz von Brown (Satz 52) lässt sich verallgemeinern (siehe Rao/Trehan [52] oder Rao [54]).

b. $M_q(g, 3)$ für $q > 2$ hat wohl zuerst Gritsenko [26] berechnet. In [26] wird für die von Rao/Trehan [52] und Neumann/Rao [47] untersuchten Generatoren g der Form $2p$, $(q-1)p$ $M_q(g, 3)$ in einer Reihe von Spezialfällen angegeben. Daneben werden noch Generatoren der Form $(q^2 \pm 1)p$, $(q-1)p^n$, $(q \pm 1)mp$ $(m < q \pm 1)$ untersucht und $M_q(g, 3)$ wird bestimmt. Die Arbeit von Gritsenko ist 1969 erschienen und damit früher als diejenigen von Rao/Trehan bzw. Neumann/Rao. Doch ist sie selbst in der 1974 erschienenen Monographie über AN-Codes von Rao [54] nicht erwähnt. Im wesentlichen ist bei Rao/Neumann op.cit. nur die Bedingung (NR) neu.

c. Im Zusammenhang mit der Arbeit von Gritsenko sind noch einige Ergebnisse über perfekte Codes zu erwähnen, die Goto/Fukumura [25] gefunden haben. Ausser diesen beiden Untersuchungen und einem frühen Resultat von Peterson [49] ist über perfekte Codes nichts weiter bekannt.

Satz 59 Sei $g = R(q) \cdot p^n$ $(n \geq 1)$, $p \neq q$ und p, q ungerade Primzahlen

$$R(q) = k.g.V.\langle 2, 3, \ldots, q-1 \rangle$$

Aus $g \mid q^\lambda - 1$, $\lambda = \omega_q(p^n)$ und $-1 \notin Z_p(q)$ folgt dann

$$g = M_q(g, 3) = q^\lambda - 1$$

Beweis Wie man leicht einsieht (etwa mit dem Bertrandschen Postulat, wie in der Bemerkung auf Seite 26 c.) gilt $R(q) > q$ für $q > 3$ und somit $g > q$ für jedes $q \geq 3$. Damit sind alle Voraussetzungen in Lemma 56 erfüllt. Aus $\alpha q^i \equiv \beta \bmod g$ $(i = 0, \ldots, \lambda - 1;$ $0 < \alpha, |\beta| < q)$ und $\alpha, \beta \mid R(q)$ sowie q Primzahl folgt $\alpha \mid \beta$ und $\beta \mid \alpha$, also $\beta = \pm \alpha$. Da $\alpha q^i \equiv \beta \bmod g$ die Kongruenz $\alpha q^i \equiv \beta \bmod p^n$ impliziert, ist $\alpha = \beta$ nicht möglich. Wir müssen noch prüfen, ob $\alpha q^i \equiv -\alpha \bmod g$, d.h. $\alpha(q^i + 1) \equiv 0 \bmod g$ möglich ist. Wegen $-1 \notin Z_p(q)$ gilt $p \nmid q^i + 1$, damit $p^{n+k} \mid \alpha$ wo $p^k \| R(q)$ $(k \geq 0)$ und dies ist ein Widerspruch, denn nach Definition des k.g.V. ist $p^{k+1} \nmid \alpha$.

Corollar 59.1 Voraussetzungen wie im vorigen Satz und -q aber nicht q ist primitive Wurzel modulo p. Dann gilt

$$g \cdot M_q^{-} (g, 3) = q^{\lambda} - 1$$

mit $\lambda = \omega_q (p^n) = \frac{p-1}{2} \cdot p^t$, $t = \text{Max}\{0, n-z\}$, $p^z \parallel (q^{\frac{p-1}{2}} - 1)$.

Beweis Vgl. Corollar 57.2.

Beispiel

a. $q = 3$, $R(3) = 2$, $g = 2p$. Da $(2, p) = 1$ genügt es $2 \mid q^{\lambda} - 1$ nachzuweisen was trivial ist weil q ungerade ist.

b. $q = 5$, $R(5) = 12$, $g = 12p$. Nun ist $12 = 3 \cdot (5-1)$ und $(p,4) = 1$ sowie $5^i \equiv (-1)^i \bmod 3$. Ist $p > 3$ so genügt es $12 \mid q^{\lambda} - 1$ nachzuweisen. $4 \mid 5^i - 1$, da $5^i \equiv 1^i \bmod 4$ und es genügt $2 \mid \lambda$ damit $12 \mid q^{\lambda} - 1$ ist. Unter den Voraussetzungen des Corollars heisst das $p \equiv 1 \bmod 4$.

Bemerkung

a. Setzt man in Satz 59 $(p, R(q)) = 1$ voraus, etwa $p > q$, so genügt es, statt $g \mid p^{\lambda} - 1$ nur $R(q) \mid q^{\lambda} - 1$ zu fordern.

b. Satz 59 geht auf eine Arbeit von Dynkin/Kimelfeld [20] zurück, in welcher Generatoren der Form $R(q) \cdot p$ eingeführt werden. Es werden in der zitierten Untersuchung die Fälle $q = 5, 7, 11$ behandelt unter der Voraussetzung q bzw. - q ist primitive Wurzel modulo p. Eine Verallgemeinerung in dieser Richtung scheint nicht möglich zu sein.

c. Auffällig an den Sätzen in diesem Abschnitt ist das Auftreten der Bedingung $-1 \notin Z_p(q)$, durch die der Fall q ist primitive Wurzel modulo p ausgeschlossen wird. Deshalb verallgemeinert Corollar 57.3 auch nur die Hälfte des Satzes von Peterson.

d. Das erstaunlichste Ergebnis unter allen Sätzen dieser Art haben Goto/Fukumura [24] , in Verallgemeinerung eines Theorems von Kondratyev/Trofimov [33], gefunden.

3.4 Fehlererkennung und -korrektur in der modularen Arithmetik

Definition 24 $R_m : \mathbb{Z}_m \longrightarrow \{0, 1, \ldots, m-1\}$ $(m \geq 1)$

$$R_m(\bar{x}) = \text{Min}\ \{y \mid y \in \bar{x},\ y \geq 0\} \quad (\bar{x} \in \mathbb{Z}_m)$$

Unter modularer Arithmetik verstehen wir die Arithmetik im Restklassenring $\mathbb{Z}_m$ $(m>1)$. Wie wir bereits aus Lemma 8 wissen, induziert jede Norm $\| \ \|_{ind}$ auf $\mathbb{Z}$ eine Norm $\| \ \|_{ind(m)}$ auf $\mathbb{Z}_m$. Es ist nun möglich ausser der durch $\| \ \|_{ind}$ induzierten Norm $\| \ \|_{ind(m)}$ unter bestimmten Voraussetzungen noch eine weitere Norm $\| \ \|^*_{ind(m)}$ auf $\mathbb{Z}_m$ zu definieren.

Definition 25

$$\|\bar{x}\|^*_{ind(m)} = \text{Min}\{\|R_m(\bar{x})\|_{ind}, \| m - R_m(\bar{x})\|_{ind}\}$$

Leider zeigt sich, dass schon $\| \ \|^*_{2(m)}$ die Bedingungen (AW2) und (AW4) verletzt.

Beispiel $m = 35$

$$\|\bar{3} + \overline{19}\|^*_{2(35)} = \|\overline{22}\|^*_{2(35)} = 3 > \|\bar{3}\|^*_{2(35)} + \|\overline{19}\|^*_{2(35)}$$
$$= 1 + 1 = 2$$

$$\|\bar{3} \cdot \overline{19}\|^*_{2(35)} = \|\overline{3 \cdot 19}\|^*_{2(35)} = \|\overline{22}\|^*_{2(35)} = 3 > \|\bar{3}\|^*_{2(35)} \cdot \|\overline{19}\|^*_{2(35)} = 1 \cdot 1 = 1$$

Weiter lässt sich auf der Menge $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ eine Metrik $d^*_{ind(m)}$ erklären.

Definition 26 $d^*_{ind(m)}(\bar{x}, \bar{y}) = \|R_m(\bar{x}) - R_m(\bar{y})\|_{ind}$ für alle $\bar{x}, \bar{y} \in \mathbb{Z}_m$ $(m>1)$

Lemma 60 $(\mathbb{Z}_m, d^*_{ind(m)})$ ist ein metrischer Raum.
Der Beweis folgt leicht aus den Eigenschaften der Norm $\| \ \|_{ind}$.
Über diese Metrik lässt sich freilich keine Norm durch $\|\bar{x}\| = d^*_{ind(m)}(0, \bar{x})$ definieren. Denn im allgemeinen ist $\|-\bar{x}\| = d^*_{ind(m)}(0, -\bar{x}) = \|R_m(-\bar{x})\|_{ind} \neq \|\bar{x}\| = \|R_m(\bar{x})\|_{ind}$.

Durch die nächsten beiden Sätze gelingt es im Fall der Norm $\| \ \|_{q(m)}$

eine Verbindung zu den Abbildungen $d^*_{q(m)}$ und $\| \ \|^*_{q(m)}$ herzustellen, die sich noch als äusserst nützlich erweisen wird.

Lemma 61 Sei $m = q^n$, $q^n + 1$, $q^n - 1$. Falls,

$(0 \leq |\alpha_i| < q) \quad \sum_{i=0}^{n-1} \alpha_i q^i \in \bar{x} \in \mathbb{Z}_m$ und $\sum(1 - \delta(\alpha_i, 0)) = s \ (s \leq n)$

so existieren Zahlen β_i mit der Eigenschaft

$$\sum_{i=0}^{n-1} \beta_i q^i \in \bar{x} \text{ und } \sum(1 - \delta(\beta_i, 0)) = s \quad (0 \leq |\beta_i| < q)$$

Beweis Aus $m = q^n$, $q^n + 1$, $q^n - 1$ folgt $q^n \equiv 0$, $q^n \equiv -1$, oder $q^n \equiv 1 \bmod m$ Durch Substitution ergibt sich die Behauptung.

Satz 62

$$m = q^n,\ q^n + 1 \text{ oder } q^n - 1 \Longrightarrow \| \ \|^*_{q(m)} = \| \ \|_{q(m)} \qquad (n > 1)$$

Beweis Aus $R_m(\bar{x}) = a$ folgt $a - m \in \bar{x}$ und zusammen mit $\|a-m\|_{q(m)} = \|m-a\|_{q(m)}$ ergibt sich $\|\bar{x}\|_{q(m)} \leq \|\bar{x}\|^*_q$ für alle $\bar{x} \in \mathbb{Z}_m$. Wir müssen noch zeigen $\|\bar{x}\|^*_{q(m)} \leq \|\bar{x}\|_{q(m)}$ für alle $\bar{x} \in \mathbb{Z}_m$. Es gilt $\|\bar{x}\|_{q(m)} \leq n$, wie man sich nach Lemma 61 leicht überlegt ($m = q^n + 1$ bietet ebenfalls keine Schwierigkeit). Der Fall $\|\bar{x}\|_{q(m)} = n$ ist trivial und es genügt $\|\bar{x}\|_{q(m)} < n$ zu betrachten. Sei $\|\bar{x}\|_{q(m)} = \|y\|_q$ mit $y \in \bar{x}$. Nach dem vorigen Lemma existieren dann ganze Zahlen $0 \leq |\beta_i| < q$, so dass gilt

$$y' = \sum_{i=0}^{n-1} \beta_i q^i \in \bar{x} \text{ und } \sum(1 - \delta(\beta_i, 0)) \leq \|y\|_q$$

woraus $\sum(1 - \delta(\beta_i, 0)) = \|y\|_q$ folgt, d.h. $\|y'\|_q = \|y\|_q$. Weiter folgt aus $|\beta_i| < q$ schon $|y'| \leq m$. Der Fall $|y'| = m$, d.h. $\bar{x} = \bar{0}$ ist trivial, da $\|\bar{0}\|^*_{q(m)} = \|\bar{0}\|_{q(m)} = 0$ klar ist. Aus $|y'| < m$ ergibt sich aber $y' = a$ oder $y' = a-m$. Also $\|y'\|_q = \|a\|_q$ oder $\|y'\|_q = \|-y'\|_q = \|m-a\|_q$. Insgesamt hat man $\|\bar{x}\|^*_{q(m)} \leq \|\bar{x}\|_{q(m)}$.

Corollar 62.1 $\| \ \|^*_{q(m)}$ ist für $m = q^n$, $q^n + 1$, $q^n - 1$ eine Norm auf $\mathbb{Z}_m$. Mit der Norm $\| \ \|^*_{q(m)}$ ist unter den Voraussetzungen von Corollar 62.1 auch eine Metrik auf $\mathbb{Z}_m$ gegeben. Ein direkter Beweis dieser Aussage ist langwierig (siehe Massey/Garcia [44], pp. 288-290). Der nächste Satz sagt aus, dass D_{min} genommen über $(\bar{g})$ in dem metrischen Raum $(\mathbb{Z}_{mg}, d^*_{q(mg)})$ gleich ist D_{min} über $(\bar{g})$ bezüglich der Norm $\| \ \|^*_{q(mg)}$, falls $mg = q^n$, $q^n + 1$, oder $q^n - 1$ gilt.

Satz 63 $mg = q^n,\ q^n \pm 1 \Longrightarrow D_{min}\left[d^*_{q(mg)}\ (\overline{g})\right] = D_{min}\left[\|\ \|^*_{q(mg)}(\overline{g})\right]$

Beweis Sei $\overline{gn} \in (\overline{g})$ und $0 < gn < gm$

$$\|\overline{gn}\|^*_{q(mg)} = \|\overline{g}\,\overline{n}\|^*_{q(mg)} = \text{Min}\left\{\|gn\|_q,\ \|mg - ng\|_q\right\}$$
$$= \text{Min}\left\{\|gn\|_q,\ \|g(m-n)\|_q\right\}$$

Nun ist $\|gn\|_q = d^*_{q(mg)}\ (\overline{gn}, \overline{0})$ und es folgt

$$D_{min}\left[d^*_{q(mg)}\ (\overline{g})\right] \leq D_{min}\left[\|\ \|^*_{q(mg)}\ (\overline{g})\right]$$

Die umgekehrte Richtung lässt sich ebenfalls leicht zeigen.

Corollar 63.1 Unter der Voraussetzung $mg = q^n,\ q^n \pm 1$ gilt

$$D_{min}\left[\|\ \|_{q(mg)}\ (\overline{g})\right] = D_{min}\left[\|\ \|^*_{q(mg)}\ (\overline{g})\right] =$$
$$= \text{Min}\left\{\|1 \cdot g\|_q,\ \|2 \cdot g\|_q,\ \ldots,\ \|(m-1)\ g\|_q\right\}$$

Beweis Für jedes Element $\overline{x},\ \overline{y} \in (\overline{g})$ gilt $R_{mg}\ (\overline{x}) = n_1\ g$, $R_{mg}\ (\overline{y}) = n_2 g,\ 0 < n_i g < mg\ (i = 1,2)$. Also

$$d^*_{q(mg)}\ (\overline{x}, \overline{y}) = \|n_1 g - n_2 g\|_q = \|n_2 g - n_1 g\|_q = \|(n_1 - n_2)\ g\|_q$$

und O.B.d.A. $n_1 \geq n_2$. Da $\|n_1 g\|_q = d^*_{q(mg)}\ (\overline{n_1 g}, \overline{0})$ haben wir gezeigt

$$D_{min}\left[d^*_{q(mg)}\ (\overline{g})\right] = \text{Min}\left\{\|1 \cdot g\|_q,\ \ldots,\ \|(m-1)\ g\|_q\right\}$$

Die Behauptung folgt dann aus Satz 62 und Satz 63.

Lemma 64 Sei $mg = q^n,\ q^n \pm 1$. Dann gilt,

$$D_{min}\left[\|\ \|_{q(mg)}\ (\overline{g})\right] \geq d \Longleftrightarrow m < M_q\ (g, d)$$

Beweis Folgt aus dem letzten Corollar und der Definition von $M_q\ (g, d)$.

Bemerkung Lemma 64 ermöglicht es uns, die Ergebnisse über $M_q\ (g,d)$ aus Abschnitt 3.3 im Fall der modularen Arithmetik im wesentlichen zu übernehmen.

Bemerkung

a. Die Aussage von Corollar 63.1 ist sehr wichtig, sie bildet die Grundlage aller bekannten Methoden zur Berechnung von D_{min}.

Das folgende Beispiel zeigt, dass diese Aussage im allgemeinen falsch ist, wenn die Voraussetzungen nicht mehr erfüllt sind.

Beispiel $m = 2$, $g = 11$, $mg = 22$, $(\overline{g}) = \{\overline{0}, \overline{11}\}$

$D_{min}[\| \|_{2(22)} (\overline{11})] = 2$, wegen $22 \cdot 46 + 11 = 1023 = 2^{10} - 1$

$D_{min}[\ d^{*}_{2(22)} (\overline{11})] = 3 = \text{Min}\{|1 \cdot 11|_2\}$

b. Da wir uns vorwiegend für die Bestimmung von D_{min} im Fall $mg = q^n - 1$ interessieren, genügt es nach Corollar 63.1 statt der Restklassen aus $(\overline{g})$ die Elemente der Form ng aus $\mathbb{Z}$ mit $0 < n \leq m-1$ bezüglich der Norm $\| \|_q$ zu betrachten.

Satz 65 Sei $mg = q^n - 1$ $(n \geq 1)$. Aus $ng = \sum_{i=0}^{n-1} \alpha_i q^i$ $(0 \leq n < m)$ folgt es existiert $0 \leq n' < m$ mit $n'g = \sum \beta_i q^i$, wobei $\beta_i = \alpha_{i-1}$ $(i \geq 1)$ und $\beta_0 = \alpha_{n-1}$ $(0 \leq \alpha_i, \beta_i \leq q-1)$ ist.

Beweis $q \cdot ng = \sum_{i=0}^{n-1} \alpha_i q^{i+1} = \alpha_{n-1} q^n + \ldots + \alpha_0 q$

Da $q^n \equiv 1 \bmod mg$ folgt $q \cdot ng \equiv \alpha_{n-2} q^{n-1} + \ldots + \alpha_0 q + \alpha_{n-1} \bmod mg$ und $0 \leq \sum_{i=0}^{n-2} \alpha_i q^{i+1} + \alpha_{n-1} < mg$. Es ist klar, dass gelten muss $g \mid (\sum \alpha_i q^{i+1} + \alpha_{n-1})$ und damit ist die Behauptung bewiesen.

Bemerkung Der vorige Satz bietet eine Erklärung dafür, warum man im Falle $mg = q^n - 1$ von "zyklischen non-separaten Restklassencodes" spricht.
Wir können nun den für die Fehlererkennung grundlegenden Satz 10 für die Norm $\| \|_{q(m)}$ aussprechen, allerdings gilt nur in den Fällen $mg = q^n$, $q^n + 1$, $q^n - 1$ eine Verschärfung wie in Satz 44.

Satz 66 Sei $mg = q^n$, $q^n \pm 1$ $(n \geq 1, q \geq 2)$. Ein non-separater Code

$$\lambda_g : \mathbb{Z}_m^+ \longrightarrow \mathbb{Z}_{mg}^+$$

kann genau dann alle Fehler aus E_c (t) korrigieren und alle Fehler aus E_d $(t + s)$ erkennen, wenn gilt

$$D_{min}[\| \|_{q(mg)} (\overline{g})] > 2t + s \quad (t, s > 0)$$

Beweis Der Beweis wird ähnlich wie in den Sätzen 10 und 44 geführt. Um die Notwendigkeit der Bedingung nachweisen zu können, muss man sich auf Corollar 63.1 stützen.

Bemerkung Aus $mg = q^n$ würde folgen $(g, q) > 1$. Lässt man die Forderung $(g, q) = 1$ fallen, so gilt falls $0 < g \leq q$ ist $D_{min} = 1$. Ist $g > q$, so zeigt ein ähnlicher Schluss wie im Beweis zu Satz 46 (iii), dass $D_{min} \leq 2$ gilt. Codes dieser Art sind also uninteressant.

Satz 67 Sei $mg = q^n - 1$, $g > q$ (also $(g, q) = 1$). Dann gilt

$$D_{min}\left[\|\ \|_{q(mg)}\ (\bar{g})\right] \geq 2$$

Beweis $\|ng\|_q = 0$, $1\ (0 < n < m) \Rightarrow ng = 0$ oder $ng = \alpha q^i$ $(i \geq 0;\ 1 \leq \alpha \leq q - 1)$ Beides ist nicht möglich.

Bemerkung Man kann auch mittels Satz 65 aus $ng = \alpha q^i$ folgern $n'g = \alpha$ für ein $0 < n' < m$, im Widerspruch zu $g > q$.

Corollar 67.1 (i) $mg = q^n - 1$, $2 | n$ und $g = q + 1 \Rightarrow D_{min} = 2$

(ii) $|(\bar{g})| = \sum_{i=1}^{n} (-1)^{i+1}\ q^{n-i}$

Beweis Nach dem vorigen Satz ist $D_{min} \geq 2$, da aus Lemma 50 $q + 1 |\ q^n - 1$ $(n \geq 1)$ folgt. Da $\|q + 1\|_q = 2$ gilt, folgt $D_{min} = 2$.

Bemerkungen

a. Die AN-Codes gemäss Corollar 67.1 können alle einfachen Fehler entdecken.

b. Aus $mg = q^n - 1$ und $\omega_q(g) < n$ folgt $n = k \cdot \omega_q(g)$ $(k > 1)$, insbesondere ist dann $q^{\omega_q(g)} - 1$ ein Codepunkt, d.h. $D_{min} = 2$. Da AN-Codes mit $D_{min} = 2$, ausgenommen $g = q-1$, uninteressant sind, setzen wir $n = \omega_q(g)$ voraus.

Um Bedingungen für $D_{min} \geq 3$ zu bekommen bei $q = 2$, brauchen wir nur die unter der Voraussetzung der unbeschränkten Integer-Arithmetik erzielten Resultate gemäss Lemma 64 zu übernehmen.

Satz 68 Sei $g \cdot m = 2^{\omega(g)} - 1$ $(g > 1)$, dann gilt

$$D_{min}\left[\|\ \|_{2(mg)}\ (\bar{g})\right] \geq 3$$

genau dann, wenn $2 \nmid \omega(g)$ oder $2 \mid \omega(g)$ und $g \nmid 2^{\omega(g)/2} + 1$.

Beweis Er folgt aus dem Satz von Brown (Satz 52), sowie Lemma 64 und Corollar 63.1.

Satz 69 Ist g = p Primzahl und ist - 2 primitives Element modulo p, aber nicht + 2, so gilt

$$D_{min}\ [\|\ \|_{2(mg)}\ (\bar{p})] = 3$$

wo $mg = 2^{\frac{p-1}{2}} - 1$ und der Code ist perfekt.

Beweis Nach Corollar 47.4 und dem vorigen Satz muss sein $D_{min} \geq 3$. Ist der Code perfekt, so haben wir mit Lemma 108 zusammen alles gezeigt. Das modulare Gewicht ≤ 1 besitzen genau die Restklassen $\bar{0}$, $\overline{2^i}$, $\overline{-2^i}$ $(0 \leq i < \frac{p-1}{2})$, also gilt $V_1 = p = g$.

Satz 70 Ist g = p Primzahl und 2 primitives Element, so gilt

$$D_{min}\ [\|\ \|_{2(mg)}\ (\bar{p})] = 3$$

$mg = 2^{\frac{p-1}{2}} + 1$ und der Code ist perfekt (und negazyklisch!).

Beispiel a. $g = 21$, $\omega(g) = 6$ $(q = 2)$

$2 \mid 6$ und $2 \nmid 2^3 + 1 \Longrightarrow D_{min} \geq 3$

$\|21\|_2 = 3$ $(21 = 1\emptyset1\emptyset1) \Longrightarrow D_{min} = 3$

b. $g = 23$ und - 2 aber nicht + 2 primitiv $(q = 2)$

$D_{min} = 3$ (Satz 69)

$m = \frac{2^{11} - 1}{23} = 89$

$Rd\ (\lambda_{23}) = \log_2 23 = 4{,}5$ (bit)

$Rt\ (\lambda_{23}) = \log_2 89 \ /\ \log_2(2^{11}-1) = 0{,}59$

Kapitel 4

Theorie der zyklischen Codes

4.1 Zyklische Permutationen

Definition 27 Die Abbildung

$$CYL_q : I_q^l \to I_q^l \quad (I_q^l = [0, q-1]^l \subset \mathbb{N}^l;\ l > 1)$$

mit $$CYL_q((\alpha_{l-1}, \ldots, \alpha_0)) = (\alpha_{l-2}, \ldots, \alpha_0, \alpha_{l-1})$$

heisst zyklische Permutation oder genauer zyklischer Linksshift (CYL : CYcle Left).

Bemerkung

a. Man überlegt sich leicht, dass CYL_q eine Permutation von I_q^l ist.

b. Bei festem q ist die Abbildung $\tilde{N} : [0, q-1]^l \to [0, q^l-1] \subset \mathbb{N}$ mit $\tilde{N}((\alpha_{l-1}, \ldots, \alpha_0)) = \sum_{i=0}^{l-1} \alpha_i q^i$ eine Bijektion. Wir werden im Folgenden diese Identifikation stillschweigend benutzen.

Definition 28 Seien g, $d \in \mathbb{N}$ $(g, d > 0)$. Dann heisst g q-zyklisch relativ zu d, wenn aus

$$g = (\alpha_{l-1}, \ldots, \alpha_0) \quad \text{(q-näre Darstellung!)}$$

folgt

$$d \mid CYL_q^n(g) \quad \text{für alle } n \geq 0.$$

Satz 71 (Bialoborski [5]) $g = (\alpha_{l-1}, \ldots, \alpha_0)$ ist dann q-zyklisch relativ zu d, wenn gilt $d \mid (g, q^l - 1)$.

Beweis $CYL_q^0(g) = g$

$$(n > 0) \qquad CYL_q^n(g) = \begin{cases} q \cdot CYL_q^{n-1}(g) \\ q \cdot CYL_q^{n-1}(g) - (q^l - 1)\,\alpha_{R_l}(l - n) \end{cases}$$

Nach Voraussetzung gilt $d \mid CYL_q^0(g)$, durch Induktion nach n folgt die Behauptung.

Bemerkung

a. Die Bedingung in Satz 71 ist nicht notwendig, wie das Beispiel $q = 10$, $l = 2$, $g = 28$ zeigt.

$$2 \nmid (28, 99)$$
$$(n \geq 0) \quad CYL_{10}^{n}(28) = \begin{cases} 28 \\ 82 \end{cases}$$

b. Die folgende Beziehung, welche man leicht dem Beweis des vorigen Satzes entnimmt, wird uns noch nützlich sein.

$$CYL_q^n(gx) = q^s \, CYL_q^{n-s}(gx) - (q^l - 1) \sum_{i=1}^{s} q^{s-i} \, \alpha_{l-n+s-i} \quad (n \geq s)$$

Corollar 71.1 $(q, d) = 1 \Longrightarrow \omega_q(d) \mid l$

Corollar 71.2 Sei $\alpha_i \in \mathbb{N}$ $(i = 0, \ldots, l-1)$ und $\sum \alpha_i > 1$. Setzen wir $q = \sum \alpha_i$, $d = q-1$ so ist $g = \sum \alpha_i q^i$ q-zyklisch relativ zu d.

Beweis
$$g = d + (g - d) = d + \left(\sum \alpha_i q^i - \sum \alpha_i\right)$$
$$= d + \sum \alpha_i (q^i - 1)$$
und $q - 1 \mid q^i - 1$ für alle $i \geq 1$.

Corollar 71.3 $g \cdot m = q^l - 1$ $(g, m > 1) \Longrightarrow gx$ ist q-zyklisch relativ zu g für alle $0 \leq x \leq m$.

Lemma 72 $(x, m) = d$ und $CYL_q^n(gx) = gx' \Longrightarrow (x', m) = d$

Beweis
$$gx' = CYL_q^n(gx) = q^n \cdot gx - (q^l - 1) \sum_{i=1}^{n} q^{n-i} \alpha_{l-i}$$

$$gx = (\alpha_{l-1}, \ldots, \alpha_0), \; q^l - 1 = mg \text{ und } (m, q) = 1$$

$$x' = q^n x - m \sum_{i \geq 1} q^{n-i} \alpha_{l-i}$$

Satz 73 Sei $(x, m) = d$ $(1 \leq x \leq m)$. Dann gilt

$$CYL_q^n(gx) = CYL_q^{n-s}(gx) = gx' \Longleftrightarrow \omega_q(m/d) \mid s$$
$(n \geq s; \; \omega_q(1) = 1)$

Beweis $\Longrightarrow$: $q^s \, CYL_q^{n-s}(gx) - CYL_q^n(gx) \equiv 0 \bmod (q^l - 1)$

$\Longrightarrow (q^s - 1) \cdot CYL_q^n (gx) \equiv 0 \bmod (q^l - 1)$

$\Longrightarrow (q^s - 1)\, x' \equiv 0 \bmod m$

$\Longrightarrow (q^s - 1)\, x'/d \equiv 0 \bmod m/d \Longrightarrow (q^s - 1) \equiv 0 \bmod m/d$

$\Longrightarrow \omega_q(m/d) \mid s$

$\Longleftarrow : \omega_q(m/d) \mid s \Longrightarrow (q^s - 1)\, CYL_q^{n-s} (gx) - (q^l - 1) \sum_{i \geq 1} q^{s-i} \alpha_{l-n+s-i} =$

$= CYL_q^n (gx) - CYL_q^{n-s} (gx) \equiv 0 \bmod (q^l - 1)$

$\Longrightarrow CYL_q^n (gx) = CYL_q^{n-s} (gx)$

Corollar 73.1 Sei $gx = (\alpha_{l-1}, \ldots, \alpha_0)$ und $(x, m) = d$. Dann folgt

$$\alpha_{l-i-\omega_q(m/d)} = \alpha_{l-i} \qquad (i \geq 1)$$

Die Indizes sind modulo l zu verstehen.

Definition 29 Sei $g \cdot m = q^l - 1$. Dann setzen wir für ein x $(0 \leq x \leq m)$

$$p_{i+1} (x) = R_m (q^i x) \text{ für } i = 0, 1, \ldots \text{ und } x \neq m$$

$$p_{i+1} (m) = m$$

und bezeichnen mit Z(x) die zyklische Klasse von x,

$$Z(x) = \{p_i(x) \mid i \geq 1\}$$

Lemma 74 $CYL_q^n (gx) = g \cdot R_m (q^n x) = g \cdot p_{n+1}(x) \quad (0 \leq x < m)$

$$CYL_q^n (gm) = gm$$

Beweis Es gilt

$$gx' = CYL_q^n (gx) = R_{q^l - 1} (q^n gx) \qquad (0 \leq x' < m)$$

$$\Longleftrightarrow x' \equiv q^n x \bmod m$$

$$\Longleftrightarrow x' = R_m (q^n x)$$

Lemma 75 $(x, m) = d \Longrightarrow d \mid p_{i+1}(x)$ für alle $i = 0, 1, 2, \ldots$

Lemma 76 $q \cdot p_i = p_{i+1} + m \cdot \alpha_{l-i} \quad (i = 1, 2, \ldots)$

und α_{l-i} ist durch diese Gleichung eindeutig bestimmt.

Beweis $q \cdot CYL_q^{i-1}(gx) = CYL_q^i(gx) + (q^l - 1)\,\alpha_{l-i}$ und das vorige Lemma.

Wir untersuchen nun die von CYL_q erzeugte zyklische Gruppe $Z(CYL_q)$, sie ist Untergruppe der symmetrischen Gruppe $\gamma_{I_q^l}$.

Lemma 77 Gilt $g \mid q^l - 1$ $(g > 1)$, so operiert $Z(CYL_q)$ auf

$$I_q^l \mid g = \{x \mid x \in I_q^l \text{ und } g \mid x\}$$

Beweis Folgt aus Corollar 71.3.

Lemma 78 Sei $(\alpha_{l-1}, \ldots, \alpha_0) \in I_q^l \mid g$, dann gilt:

(i) $\alpha_{l-i} = R_q(R_{q^l-1}(q^i gx))$, $gx = (\alpha_{l-1}, \ldots, \alpha_0)$

(ii) $g \equiv 1 \bmod q \Longrightarrow \alpha_{l-i} = R_q(R_m(q^i x))$ $(0 \leq x < m)$

Satz 79 Sei $mg = q^l - 1$ $(g, m > 1, q < m)$, dann gibt es zu jedem Teiler d von m genau $\varphi(m/d)/\omega_q(m/d)$ Orbits (Transitivitätsgebiete) von $Z(CYL_q)$ auf $I_q^l \mid g$ mit $\omega_q(m/d)$ Elementen $(\omega_q(1) = 1)$.

Insgesamt gibt es

$$N = 1 + \sum_{d \mid m} \frac{\varphi(m/d)}{\omega_q(m/d)}$$

Orbits, darunter die trivialen Orbits, den Nullorbit $\{(0, \ldots, 0)\}$ und den Einsorbit $\{(1, \ldots, 1)\}$. Die nichttrivialen Orbits sind im wesentlichen durch die verschiedenen Nebenklassen der von $\bar{q}$ in $E(\mathbb{Z}_{m/d})$ (Einheitengruppe des Ringes $\mathbb{Z}_{m/d}$) erzeugten zyklischen Gruppe bestimmt.

Beweis Aus Lemma 72 folgt, dass falls gx und gx' $(0 \leq x, x' < m)$ in einem Orbit liegen $(x, m) = (x', m) = d$ gilt. Aus Satz 73 sowie Corollar 73.1 ergibt sich, dass jeder Orbit genau $\omega_q(m/d)$ Elemente enthält. Nach Lemma 74 liegen gx und gx' genau dann in demselben Orbit, wenn x und x' in derselben zyklischen Klasse liegen. Aus Lemma 76 folgt, dass die zyklischen Klassen, bis auf den Faktor d, mit den Nebenklassen von $\bar{q}$ in $E(\mathbb{Z}_{m/d})$ übereinstimmen.

Die Anzahl der verschiedenen zyklischen Klassen zu einem vorgegebenen d|m ist dann gerade der Index der zyklischen Gruppe $Z(\overline{q})$ in $E(\mathbb{Z}_{m/d})$, also $\varphi(m/d) / \omega_q(m/d)$, woraus die Formel für N folgt (mit dem zusätzlichen Summanden 1 wird die "Nullklasse" berücksichtigt).

Satz 80 Seien $\overline{gx}_1$, $\overline{gx}_2 \in (\overline{g}) \subset \mathbb{Z}_{mg}$, $mg = q^l - 1$ $(0 \neq x_1, x_2 \neq m;\ l > 1)$

Es gilt:

(i) Liegen $R_{mg}(gx_1)$ und $R_{mg}(gx_2)$ im gleichen Orbit in $I_q^l|g$, so folgt

$$\|\overline{gx}_1\|^*_{q(mg)} = \|\overline{gx}_2\|^*_{q(mg)}$$

(ii) Sind gx_i $(i = 1, \ldots, N-2)$ Repräsentanten aus den nichttrivialen Orbits von CYL_q auf $I_q^l|g$, so ist

$$D_{min} = \operatorname{Min}\left\{\|\overline{gx}_i\|^*_{q(mg)} \mid i = 1, \ldots, N-2\right\}$$

Beweis (i) Zum Beweis braucht man vor allem Lemma 23, es gilt danach

$$\|\overline{q}\ \overline{gx}\|_{q(q^l-1)} = \|\overline{gx}\|_{q(q^l-1)}$$

und dies ist wegen Satz 62 auch für die Norm $\|\ \|^*_{q(q^l-1)}$ richtig. Dem vorigen Satz kann man entnehmen, dass alle Elemente eines Orbits sich modulo $q^l - 1$ als $\overline{q}^i\ \overline{gx}$ schreiben lassen, woraus schon alles folgt.

(ii) Dies ist eine einfache Folgerung aus (i).

Bemerkung Es sei angemerkt, dass wir statt der hier gewählten Darstellung auch mit Shift-Registern hätten arbeiten können. In Definition 27 wird ja nichts anderes als ein zirkuläres Shift-Register algebraisch definiert.

Corollar 80.1 Ist m = p Primzahl, $q \prec p$ primitives Element modulo p, so ist der AN-Code $\lambda_g : \mathbb{Z}_p^+ \longrightarrow \mathbb{Z}_{pg}^+$ äquidistant $(pg = q^l - 1)$.

Beweis Nach Voraussetzung ist $\omega_q(p) = p - 1$, also $p - 1 \mid l$. Es gilt $N - 2 = 1$, d.h. es existiert nur ein nicht-trivialer Orbit

in $I_q^1|g$ bezüglich $Z(CYL_q)$. Alles weitere folgt aus dem vorigen Satz.

Beispiele

a. $m = 9$, $g = 7$, $mg = 2^6 - 1 = 63$

Orbitstruktur: $\omega_2(9) = 6$, $\varphi(9) = 6$

$d = 1$:

ØØØ111	$1 \cdot 7$
ØØ111Ø	$2 \cdot 7$
Ø111ØØ	$2^2 \cdot 7$
111ØØØ	$2^3 \cdot 7$
11ØØØ1	$7 \cdot 7 \equiv 2^4 \cdot 7 \bmod 63$
1ØØØ11	$5 \cdot 7 \equiv 2^5 \cdot 7 \bmod 63$
ØØØ111	$1 \cdot 7 \equiv 2^6 \cdot 7 \bmod 63$

$d = 3$:

Ø1Ø1Ø1	$3 \cdot 7$
1Ø1Ø1Ø	$6 \cdot 7 = 2 \cdot 3 \cdot 7$
Ø1Ø1Ø1	$3 \cdot 7 \equiv 2^2 \cdot 3 \cdot 7 \bmod 63$

$\varphi(9/3) = 2$
$\omega_2(3) = 2$

b. $m = 5$, $g = 3$, $mg = 2^4 - 1 = 15$

Orbitstruktur: $\omega_2(5) = 4$, $\varphi(5) = 4$ und 5 ist Primzahl

ØØ11	$1 \cdot 3$
Ø11Ø	$2 \cdot 3$
11ØØ	$2^2 \cdot 3$
1ØØ1	$3 \cdot 3 \equiv 2^3 \cdot 3 \bmod 15$
ØØ11	$4 \cdot 3 \equiv 2^4 \cdot 3 \bmod 15$

Satz 81 Sei $(m/d), q-1) = 1$, wo $d = (m, x)$ ist. Dann gilt.

$$\sum_{i=1}^{\lambda} p_i(x) = m \cdot K(x) \qquad (0 < x < m)$$

$$\sum_{i=1}^{\lambda} \alpha_{1-i}(x) = (q-1) \cdot K(x)$$

mit $\lambda = \omega_q(m/d)$. $K(x)$ ist eine natürliche Zahl.

Beweis $x = m$ ist klar ($\omega_q(1) = 1$).

Aus

$$q \cdot CYL_q^{n-1}(gx) = CYL_q^n(gx) + (q^1 - 1)\alpha_{1-n}$$

folgt durch Summation

$$q \cdot \sum_{i=1}^{\lambda} CYL_q^{i-1}(gx) = \sum_{i=1}^{\lambda} CYL_q^i(gx) + (q^1 - 1)\sum_{i=1}^{\lambda} \alpha_{1-i}$$

Nach Satz 73 gilt $\sum_i CYL_q^{i-1}(gx) = \sum_i CYL_q^i(gx)$, also

$$(q-1)\sum CYL_q^{i-1}(gx) = (q^1 - 1)\sum \alpha_{1-i}$$

$$(q-1) \cdot g \cdot \sum p_i(x) = m \cdot g \cdot \sum \alpha_{1-i} \qquad (d \mid \sum p_i!)$$

woraus die Behauptung folgt.

Corollar 81.1

$$\sum_{i=1}^{l} p_i(x) = m \cdot K(x) \cdot \frac{1}{\omega_q(m/d)}$$

$$\sum_{i=1}^{l} \alpha_{1-i}(x) = (q-1) \cdot K(x) \cdot \frac{1}{\omega_q(m/d)}$$

Beweis Nach Satz 73 und Corollar 73.1

Corollar 81.2 Ist $m = p$ ungerade Primzahl und q primitives Element, sowie $p \nmid q-1$, dann ist $K(x) = \frac{1}{2}\omega_q(p)$ $(1 \leq x < p)$

Beweis

$$\sum p_i(x) = \sum_{i=1}^{p-1} i = \frac{1}{2} p (p - 1)$$

Satz 82 Sei $s \cdot f = \omega_q(m/d)$, $(x, m) = d$ und $(m/d, q^f - 1) = 1$.
Dann gelten die Beziehungen:

$$\sum_{i=0}^{s-1} p_{r+i \cdot f} = m \cdot k_r \qquad (r = 1, 2, \ldots, f)$$

$$\sum_{i=0}^{s-1} \alpha_{1-r-i \cdot f} = q \cdot k_r - k_{r+1} \qquad (0 < x < m)$$

und k_r ist eine natürliche Zahl mit $1 \leq k_r \leq s - 1$, sowie $k_{f+1} = k_1$.

Beweis Ist f = 1, so folgt alles aus Satz 81.

$$c \cdot m/d = q^{\lambda} - 1 = (q^f - 1) \sum_{i=0}^{s-1} q^{i \cdot f} \Longrightarrow \frac{m}{d} \mid \sum q^{i \cdot f}$$

$$\Longrightarrow m \mid p_r \sum q^{i \cdot f} \text{ (wegen } d \mid p_r \text{ nach Lemma 75)}$$

$$p_r \sum q^{i \cdot f} \equiv \sum p_{r+i \cdot f} \bmod m \quad (1 \leq r \leq f)$$

Also

$$\sum p_{r+i \cdot f} = m \cdot k_r$$

für eine ganze Zahl k_r. Aus $1 \leq p_r < m$ folgt:

$$1 \leq k_r \leq s - 1$$

Alles weitere folgt aus Lemma 76. Die Fälle x = 0 bzw. x = m lassen sich auch durch die Gleichungen beschreiben, freilich mit $k_r = 0$ bzw. $k_r = s$ für alle r.

Corollar 82.1 $s \cdot f = \omega_q(m/d)$, $(m/d, q^f - 1) = 1$ und $mg = q^l - 1$.

Nun ist $l = s \cdot f \cdot \frac{l}{\omega_q(m/d)} = s' \cdot f$ und man folgert leicht aus dem vorigen Satz:

$$\sum_{i=0}^{s'-1} p_{r+i \cdot f} = m \cdot k_r \cdot \frac{l}{\omega_q(m/d)}$$

$$\sum_{i=0}^{s'-1} \alpha_{l-r-i \cdot f} = \frac{l}{\omega_q(m/d)} \quad (q \cdot k_r - k_{r+1})$$

Satz 83 Ist F der grösste echte Teiler von $\omega_q(m/d)$ für den gilt $(q^F - 1, m/d) = 1$, so genügt die in Satz 81 definierte Konstante K(x) der Ungleichung:

$$F \leq K(x) \leq \omega_q(m/d) - F \qquad (0 < x < m)$$

Beweis Nach Satz 82 gilt $1 \leq k_r \leq \omega_q(m/d)/f - 1$ $(r = 1, 2, \ldots, f)$. Summation ergibt

$$f \leq \sum k_r \leq \omega_q(m/d) - f$$

Nach Satz 82

$$m \sum k_r = \sum p_i = m \cdot K(x)$$

und die Behauptung folgt.

Corollar 83.1 Ist $\omega_q(m/d)$ gerade, so wird $F = \omega_q(m/d) / 2 = \lambda/2$ und es gilt

$$K = \frac{1}{2} \omega_q(m/d)$$

$$\text{(KC)} \quad \begin{aligned} p_r + p_{r+\lambda/2} &= m \\ \alpha_{l-r} + \alpha_{l-r-\lambda/2} &= q - 1 \end{aligned}$$

unter der Voraussetzung $(m/d, q^{\lambda/2} - 1) = 1$.

Definition 30 Gilt $g \cdot m = q^l - 1$ und erfüllt ein x $(0 < x < m)$ die Bedingungen (KC) in Corollar 83.1, so sagen wir x gehört zur Klasse C.

Bemerkung Eine notwendige Bedingung damit x zur Klasse C gehört ist trivialerweise $2 \mid \omega_q(m/d)$.

Satz 84 Die folgenden Bedingungen sind hinreichend dafür, dass x zur Klasse C gehört:

(i) $(m/d, q^{\lambda/2} - 1) = 1$, $\lambda = \omega_q(m/d)$, $(x, m) = d$.

(ii) $m = p^\alpha$ ($p > 2$, Primzahl) und q ist primitives Element.

(iii) $\varphi(m/d) / \omega_q(m/d)$ ist ungerade.

(iv) $m = p^\alpha$ ($p > 2$, Primzahl) und $2 \mid \omega_q(m/d)$.

Für den Beweis benötigen wir noch zwei Lemmata.

Lemma 85 Notwendig und hinreichend damit $0 < x < m$ zur Klasse C gehört ist die Bedingung

$$m - x \in Z(x)$$

Beweis Die Notwendigkeit ist klar. Umgekehrt folgt aus $p_r(x) = m - x \in Z(x)$ $(r > 1)$,

$$p_i + p_{i+r-1} = m \quad (i = 1, 2, \ldots, r - 1)$$

was leicht aus der Definition der p_i zu ersehen ist.

Aus $q \cdot p_i = p_{i+1} + m \cdot \alpha_{l-i}$ ergibt sich dann,

$$q\,(m-p_i) = (m - p_{i+1}) + m\,(q-1-\alpha_{l-i})$$

$$q \cdot p_{i+r-1} = p_{i+r} + m \cdot (q-1-\alpha_{l-i})$$

d.h. $\alpha_{l-i} + \alpha_{l-i-(r-1)} = q - 1$

und $\omega_q(m/d) = 2(r-1)$

Bemerkung Aus Lemma 85 kann man schliessen: ein x mit $(x, m) = d$ gehört genau dann zur Klasse C, wenn $q^r \equiv -1 \bmod m/d$ für ein $r \geq 1$ gilt. Die Eigenschaft zu Klasse C zu gehören ist demnach nur von q und m/d abhängig, d.h. gehört ein x mit $(x, m) = d$ zur Klasse C, so auch schon alle x mit dieser Eigenschaft. Wir sagen q gehört modulo m/d zur Klasse C.

Lemma 86 Es gelte $(x, m) = d$, $2 \mid \omega_q(m/d)$, $q^{\lambda/2} \equiv -1 \bmod m/d$. Dann gehört q modulo m/d zur Klasse C. Die Umkehrung gilt ebenfalls.

Beweis zu Satz 84

(i) Corollar 83.1

(ii) Lemma 85 und die anschliessende Bemerkung.

(iii) Gilt $m - x \notin Z(x)$, so $p_i(x) + p_i(m-x) = m$ $(i \geq 1)$ $((x, m) = d)$ und $Z(x) \cap Z(m-x) = \phi$. Da $\varphi(m/d)/\omega_q(m/d)$ die Anzahl der verschiedenen Z(x) mit $(x, m) = d$ ist, so muss diese Zahl gerade sein. Ist sie ungerade, so muss ein x zur Klasse C gehören und damit alle x.

(iv) $\varphi(m/d) = p^{\alpha-i}(p-1) \Longrightarrow \omega_q(m/d) = p^{\alpha-j}(p-1)$ $(j \geq i \geq 0)$

$\Longrightarrow \varphi(m/d) / \omega_q(m/d) = p^{j-i}$

$2 \nmid p^{j-i}$ und nach (iii) gilt die Behauptung.

Lemma 87 Ist $m = p$ Primzahl $(p > 2)$, so gehört q modulo m genau dann zu C, wenn $\omega_q(p)$ gerade ist.

Beweis $\Longrightarrow$: Aus $2 \mid \omega_q(p)$ folgt $(q^{\lambda/2} - 1)(q^{\lambda/2} + 1) \equiv 0 \bmod p$, d.h. aber $(q^{\lambda/2} - 1, p) = 1$. Aus Satz 84 (i) folgt die Behauptung.
$\Longleftarrow$: Gehört q modulo m zu C, so muss notwendig $q^r \equiv -1 \bmod p$ $(r \geq 1)$ gelten. Weiter impliziert dies $q^{2r} \equiv 1 \bmod p$, also $\omega_q(p) \mid 2r$ und aus $2 \nmid \omega_q(p)$ folgt $\omega_q(p) \mid r$. Demnach $q^r \equiv 1 \bmod p$, d.h. $2 \equiv 0 \bmod p$. Es muss also gelten $2 \mid \omega_q(p)$ und weiter wie gehabt.

Corollar 87.1 Sei m = p ungerade Primzahl. Gilt $q^{\frac{p-1}{2}} \equiv -1 \bmod p$, so gehört q modulo p zu C.

Bemerkung Da $g \cdot m = q^l - 1$, so kann man jeden Codepunkt gx eines zyklischen Codes als $\frac{x}{m} \cdot (q^l - 1)$ schreiben. Ist $(x, m) = 1$ dann besitzt, wegen $(q, m) = 1$, $\frac{x}{m}$ entwickelt zur Basis q eine rein periodische q-näre Darstellung $0, \dot{a}_1 \ldots \dot{a}_\lambda$ $(\lambda = \omega_q(m))$.
Für q = 10 haben wir es mit einem periodischen Dezimalbruch zu tun. Diese einfache aber weittragende Entdeckung wurde schon von Mandelbaum [42] gemacht, welcher in der zitierten Arbeit die zyklischen Codes einführte. Die Partition der Codepunkte gemäss Satz 79 wurde von Tsao-Wu [66] in seiner Dissertation eingeführt. Unsere Darstellung geht von Satz 71 aus, den Bialoborski [5] aufstellte. Er gestattet es, die gesamte Theorie ohne Rückgriff auf die periodische q-näre Entwicklung des Bruches $\frac{x}{m}$ aufzuziehen. Die Sätze dieses Abschnitts erhält man durch übertragen von bekannten Sätzen über periodische Dezimalbrüche (siehe z.B. Batty [4], Leavitt [35]). Der gesamte bisher aufgebaute Apparat soll uns dazu dienen, obere und untere Schranken für D_{min} zu gewinnen.

Satz 88 Sei $m \cdot g = 2^l - 1$ und eine der folgenden Bedingungen erfüllt:

(i) $(m/d, 2^{\lambda/2} - 1) = 1$, mit $\lambda = \omega_2(m/d)$, für alle $d \mid m$.

(ii) $m = p^\alpha$ (p ungerade Primzahl) und 2 ist primitives Element.

(iii) $\varphi(m/d) / \omega_2(m/d)$ ist ungerade für alle $d \mid m$.

(iv) $m = p^\alpha$ $(p > 2$, Primzahl) und $2 \mid \omega_2(m/d)$ für alle $d \mid m$.

(Wir können stets $d \neq m$ fordern).

Dann gilt

$$D_{min}\left[\|\ \|_{2(mg)}\ (\bar{g})\right] \leq 1/2$$

Beweis Nach Satz 84 gehört 2 modulo m/d für alle d|m zur Klasse C. Es muss deshalb in der binären Darstellung eines jeden Repräsentanten der verschiedenen Orbits an genau 1/2 Stellen eine "1" stehen.

4.2 Abschätzung von D_{min}

Um untere Schranken für D_{min} zu gewinnen, legen unsere bisherigen Untersuchungen zusammen mit Corollar 103.1 das folgende Verfahren nahe. Wir bestimmen kleinste Repräsentanten aus den nichttrivialen Orbits und schätzen ihr Gewicht nach unten ab, dazu benutzen wir Satz 42. Das Minimum genommen über diese Schranken ist dann eine untere Schranke für D_{min}. Einfachster Fall ist $m \cdot g = q^{\lambda} - 1$, wo $m = p^n$ $(n \geq 1)$, $\lambda = \omega_q(m)$ und q ist primitives Element modulo m. Kleinste positive Repräsentanten sind dann $g \cdot p^i$ $(i = 0, \ldots, n-1)$. Wir beweisen zunächst einen Satz, der eine allgemeine Aussage über die Anzahl $N_q(B_j, m)$ von Blöcken $B_j(m) = (\beta_{j-1}, \ldots, \beta_0)$ $(0 \leq \beta_k \leq q-1;\ k = 0, \ldots, j-1)$ der Länge j in $\frac{q^{\lambda}-1}{m} = g$

$$= (\alpha_{\lambda-1}, \ldots, \alpha_0)$$

macht.

Satz 89 Sei $2 \leq q < p^n$ $(n \geq 1)$ primitive Wurzel modulo p^2, wo $p > 2$ eine Primzahl ist. Dann bestimmt sich die Häufigkeit mit der ein Block B_j (p^n) von j Zahlen aus der Menge $\{0, 1, 2, \ldots, q-1\}$ in der q-nären Darstellung $(\alpha_{\lambda-1}, \ldots, \alpha_0)$ von $\frac{q^{\lambda}-1}{m} = g$ $(\lambda = \varphi(p^n))$ erscheint durch

$$N_q\ (B_j,\ p^n) = \left[\frac{p^n}{q^j}\right] - \left[\frac{p^{n-1}}{q^j}\right] + \xi_q\ (p^n)$$

wo $|\xi_q| \leq 2$ und $j \leq \left[n \log_q p\right]$. Die Werte von ξ_q als Funktion von n und j sind durch die folgende Tabelle gegeben:

n	j	ε_q
1	1	$\emptyset$, 1
1	$2 \leq j \leq \lceil \log_q p \rceil$	-1, $\emptyset$, 1
>1	1	-1, $\emptyset$, 1
>1	$2 \leq j \leq \lceil n \log_q p \rceil$	-2, $\emptyset$, 1

Gilt $\lceil n \log_q p \rceil - j \leq \lambda$, so ist $N_q(B_j, p^n) = \begin{cases} \emptyset \\ 1 \end{cases}$

Beweis $\frac{q^\lambda - 1}{p^n} = g = (\alpha_{\lambda-1}, \ldots, \alpha_{\lambda-k}, \ldots, \alpha_{\lambda-k-j+1}, \ldots, \alpha_0)$

$B_j = (\alpha_{\lambda-k}, \ldots, \alpha_{\lambda-k-j+1})$

Es gilt $CYL_q^{k-1}(g) = g \cdot p_k$ und daraus folgt

$$B_j = \left\lfloor \frac{g \cdot p_k}{q^{\lambda-j}} \right\rfloor = \left\lfloor \frac{p_k q^j}{m} \cdot \frac{q^\lambda - 1}{q^\lambda} \right\rfloor$$

$$= \left\lfloor \frac{p_k \cdot q^j}{m} \left(1 - \frac{1}{q^\lambda}\right) \right\rfloor$$

Wir müssen $k \geq \lambda - j + 1$ voraussetzen, was $p_k \leq q^{\lambda-j}$ bedeutet (man beachte, dass die Umkehrung nicht gilt, siehe weiter unten). Nun folgt

$$\frac{p_k \cdot q^j}{m} \cdot \frac{1}{q} \leq \frac{1}{m} \quad \text{und weil } m \nmid p_k q^j, \text{ so}$$

$$B_j = \left\lfloor \frac{p_k \cdot q^j}{m} \right\rfloor$$

Weiter schliessen wir

$$0 \leq \frac{m \cdot B_j}{q^j} < p_k < \frac{m \cdot (B_j + 1)}{q^j} \leq m \quad \text{oder} \quad p_k \in I_1 = \left(\frac{m \cdot B_j}{q^j}, \frac{m \cdot (B_j + 1)}{q^j} \right)$$

Wir müssen um unser Ziel zu erreichen demnach alle p_k in dem angegebenen Intervall bestimmen, dies sind alle Zahlen in dem Intervall welche relativ prim zu p sind. Diejenigen Zahlen welche nicht relativ prim zu p sind liegen in dem Intervall:

$$I_2 = \left(\frac{m \cdot B_j}{p \cdot q^j} , \frac{m \cdot (B_j+1)}{p \cdot q^j} \right)$$

Durch Fallunterscheidung erhalten wir die verschiedenen Lösungen des Problems, zuerst für $n > 1$.

a. $B_j = 0$

$$I_1 = \left(0, \frac{m}{q^j}\right)$$

$$I_1' = \left(0, \frac{m}{p \cdot q^j}\right)$$

$$N_q(B_j, m) = \left[\frac{m}{q^j}\right] - \left[\frac{m}{p \cdot q^j}\right]$$

b. $B_j = q^j - 1$

$$I_1 = \left(m - \frac{m}{q^j} , m \right)$$

$$I_2 = \left(\frac{m}{p} - \frac{m}{p \cdot q^j} , \frac{m}{p}\right)$$

$$N_q(B_j, m) = \left[\frac{m}{q^j}\right] - \left[\frac{m}{p \cdot q^j}\right]$$

c. $B_j \neq 0,\ q^j - 1$

$$N_q(B_j, m) = \left[\frac{m\ (B_j+1)}{q^j}\right] - \left[\frac{m\ B_j}{q^j}\right] - \left\{\left[\frac{m \cdot (B_j+1)}{p \cdot q^j}\right] - \left[\frac{m \cdot B_j}{p \cdot q^j}\right]\right\}$$

Dies gilt deshalb, weil $q^j \nmid m\ (B_j+1)$, mB_j, $\frac{m}{p}\ (B_j+1)$, $\frac{m}{p}\ B_j$ (entsprechende Überlegungen haben wir auch in a. und b. stillschweigend benutzt).

Aus

$$[a + b] = \begin{cases} [a] + [b] \\ [a] + [b] + 1 \end{cases}$$ ergibt sich

$$N_q(B_j, m) = \left[\frac{m}{q^j}\right] - \left[\frac{m}{p \cdot q^j}\right] + \varepsilon_q(m)$$

$$\varepsilon_q(m) = -1, \emptyset, 1.$$

Im Fall n = 1 führen entsprechende Überlegungen auf die Formel

$$N_q(B_j, m) = \left[\frac{p}{q^j}\right] + \varepsilon_q(p)$$

$$\varepsilon_q(p) = \emptyset, 1$$

Es dürfte klar sein, dass $N_q(B_j, m) = \begin{cases} \emptyset \\ 1 \end{cases}$ für $\left[n \log_q p\right] < j \leq p^{n-1}$ $(p - 1)$ denn in diesem Fall ist $\frac{m}{q^j} < 1$. Sei also $2 \leq j \leq \left[n \log_q p\right]$, dann müssen wir noch eine Korrektur bei unserer Zählung vornehmen. Sie betrifft diejenigen Blöcke B_j, welche mit α_k beginnen, wobei $k < \lambda - j+1$ gilt. Diese Blöcke laufen zyklisch zurück in den Anfang von g hinein, evemtuell haben wir einige von ihnen mitgezählt. Nun beginnt g mit einem Block von $j = \left[n \log_q p\right]$ Nullen, d.h. zyklisch laufende Blöcke enden mit Nullen. Zu jedem $j \geq 2$ gibt es nun $j - 1$ derartiger Blöcke, die wegen der verschiedenen Anzahl von Nullen am Blockende auch verschieden sind. Es sei denn am Ende von g würde gelten $\alpha_i = 0$ für alle $i \leq k < \lambda - j+1$, dies ist wegen $(g, q) = 1$ nicht möglich. Wir können aus allem schliessen, dass wir höchstens einen Block zuviel gezählt haben können. Dies berücksichtigen wir durch

$$\varepsilon_q(m) = -1, \emptyset, 1 \text{ für } n = 1 \; j > 1$$

$$\varepsilon_q(m) = -2, -1, \emptyset, 1 \text{ für } n > 1, \; j > 1$$

Ist $j = 1$, so kann natürlich nichts passieren.

Bemerkung Satz 89 stammt von Stoneham [62] und wurde für periodische q-adische Brüche $\frac{1}{p^n}$ bewiesen. Wir benötigen den Beweis um den nächsten Satz abzuleiten. Man beachte, dass Blöcke, die sich überlappen, getrennt gezählt werden.

Satz 90 Sei $2 \leq q < p$ primitive Wurzel modulo p^2 (p Primzahl). Weiter gelte $g \cdot m = q^{\lambda} - 1$ mit $m = p^n (n \geq 1), \lambda = \varphi(p^n) = p^{n-1}(p-1)$ und $2 \nmid [\log_q p]$. Dann gilt:

$$D_{min}\left[\| \|_{q(mg)}(\bar{g})\right] \geq \text{Min}\left\{SB_2(m),\ p \cdot SB_2\left(\frac{m}{p}\right),\ \ldots,\ p^{n-1} \cdot SB_2\left(\frac{m}{p^{n-1}}\right)\right\}$$

$$SB_2\left(\frac{m}{p^k}\right) = \sum_{i=1}^{q-1}\left(\left[\frac{m(1+i)}{p^k \cdot q^2}\right] - \left[\frac{m \cdot i}{p^k \cdot q^2}\right] - \left\{\left[\frac{m(1+i)}{p^k \cdot p \cdot q^2}\right] - \left[\frac{m \cdot i}{p^k \cdot p \cdot q^2}\right]\right\}\right) \quad (k = 0, \ldots, n-1)$$

Beweis Wir bestimmen nach den Methoden im Beweis des vorigen Satzes $N_q(B_2, m/p^k)$, wo $B_2 = (\emptyset, z)$ $(1 \leq z \leq q-1)$ ist. Dabei ist zu beachten, dass weder überlappen noch zyklisches Zurücklaufen passieren können.

Beispiel $m = 5^2$, $q = 2$

$2 \leq [\log_2 5]$, $\omega_2(25) = 20$, $g = 41\,943$, $mg = 2^{20} - 1 = 1\,048\,575$

$g \cdot 1 = (\emptyset\emptyset\emptyset\emptyset 1\emptyset 1\emptyset\emptyset\emptyset 1111\emptyset 1\emptyset 111)$

$g \cdot 5 = (\emptyset\emptyset 11\emptyset\emptyset 11\emptyset\emptyset 11\emptyset\emptyset 11\emptyset\emptyset 11)$

$\|g\|_2 = 6$, $\|g \cdot 5\|_2 = 10$ also $D_{min} = 6$

$$SB_2(25) = \left[\frac{25 \cdot 2}{4}\right] - \left[\frac{25 \cdot 1}{4}\right] - \left\{\left[\frac{5 \cdot 2}{4}\right] - \left[\frac{5 \cdot 1}{4}\right]\right\}$$

$$= 12 - 6 - 2 + 1 = 5$$

$$SB_2(5) = \left[\frac{5 \cdot 2}{4}\right] - \left[\frac{5 \cdot 1}{4}\right] - \left\{\left[\frac{2}{4}\right] - \left[\frac{1}{4}\right]\right\}$$

$$= 1$$

$5 \cdot SB_2(5) = 5$

Also $D_{min} \geq 5$.

Wir sind jetzt in der Lage auch obere Schranken für D_{min} im Fall

$q > 2$ abzuleiten und für $q = 2$ die in Satz 88 angegebene Schranke noch zu verbessern.

Satz 91 Sei $2 \leq q < p$ primitive Wurzel modulo p^2 (p Primzahl). Weiter gelte $g \cdot m = q^{\lambda} - 1$, mit $m = p^n$ ($n \geq 1$), $\lambda = p^{n-1}(p-1)$. Dann gilt

$$D_{min}\left[\|\ \|_{q(mg)}\ (\bar{g})\right] = \text{Min}\left\{ UB\left(\frac{m}{p^k}\right) \;\middle|\; k = 0, \ldots, n-1 \right\}$$

$$UB\left(\frac{m}{p^k}\right) = \|g \cdot p^k\|_H - p^k \sum_{r \geq 3} (r-2)\, NB_{r+2}\left(\frac{m}{p^k}\right)$$

$$NB_{r+2}\left(\frac{m}{p^k}\right) = \left(\left\{ \left[\frac{m \cdot \left(1 + \sum_{i=1}^{r} (q-1)\, q^i\right)}{p^k \cdot q^{r+2}} \right] - \left[\frac{m \cdot \sum_{i=1}^{r} (q-1)\, q^i}{p^k \cdot q^{r+2}} \right] \right\} - \left\{ \left[\frac{m \cdot \left(1 + \sum_{i=1}^{r} (q-1)\, q^i\right)}{p^k \cdot p \cdot q^{r+2}} \right] - \left[\frac{m \cdot \sum_{i=1}^{r} (q-1)\, q^i}{p^k \cdot p \cdot q^{r+2}} \right] \right\} \right)$$

Beweis Folgt aus Satz 89 und der Bemerkung c. nach Satz 41. Man hat noch zu beachten, dass Blöcke der Form 0 q-1 q-1 ... q-1 0 sich nur "unwesentlich" überlappen können und zyklisches Zurücklaufen auch keine Korrektur nötig macht.

Corollar 91.1 Unter denselben Voraussetzungen wie im vorigen Satz und $q = 2$ kann man $\|g \cdot p^k\|_H$ durch die Konstante $\lambda/2$ ersetzen.

Beweis Nach Satz 88.

Beispiel Wir nehmen das letzte Beispiel wieder auf.

$$NB_5(25) = \left[\frac{25 \cdot 15}{32}\right] - \left[\frac{25 \cdot 14}{32}\right] - \left\{ \left[\frac{5 \cdot 15}{32}\right] - \left[\frac{5 \cdot 14}{32}\right] \right\}$$

$$= 11 - 10 - \{ 2 - 2 \}$$

$$= 1$$

$$NB_6(25) = \left[\frac{25 \cdot 31}{64}\right] - \left[\frac{25 \cdot 30}{64}\right] - \left\{ \left[\frac{5 \cdot 31}{64}\right] - \left[\frac{5 \cdot 30}{64}\right] \right\}$$

$$= 12 - 11 - \{ 2 - 2 \}$$

$$= 1$$

$NB_{r+2}(25) = 0$ für alle $r \geq 5$.

$NB_{r+2}(5) = 0$ für alle $r \geq 3$.

$D_{min} \leq 10 - 3 = 7$, insgesamt : $5 \leq D_{min} \leq 7$

Bemerkung Satz 90 und Corollar 91.1 sind für $m = p$, $q = 2$ indirekt zuerst von Mandelbaum [42] benutzt worden um untere und obere Schranken für D_{min} abzuleiten. Wie wir noch sehen werden, lässt sich D_{min} exakt bestimmen. Es dürfte klar sein, wie man verfahren muss, wenn $g \cdot m = q^l - 1$ und $l = k \cdot \lambda$ $(k > 1)$ gilt.
Mit Hilfe der Theorie der Totative (vgl. Holzer [30]) lassen sich in einigen Fällen handlichere Abschätzungen gewinnen.

Satz 92 Sei $2 \leq q^2 < p$ und q primitive Wurzel modulo p^2 (p Primzahl) Weiter gelte $g \cdot m = p^\lambda - 1$, mit $m = p^n$ $(n \geq 1)$, $\lambda = p^{n-1}(p-1)$ und $2 \nmid [\log_q p]$. Dann gilt:

(i) Für $p \equiv 1 \bmod q^2$

$$D_{min} \geq \frac{\varphi(p^n)}{q^2} \cdot (q-1) = \frac{p^{n-1}(p-1)}{q^2}(q-1)$$

(ii) Für $m = p$ und $p \equiv -1 \bmod q^2$

$$D_{min} \geq \frac{p+1}{q^2}(q-1)$$

Beweis In Satz 90 bedeutet $SB_2\left(\frac{m}{p^k}\right)$ die Summe aller Totative von $\frac{m}{p^k}$ in den Intervallen $\left(\frac{m(1+i)}{p^k \cdot q^2}, \frac{m \cdot i}{p^k \cdot q^2}\right)$ $(i = 1, \ldots, q-1)$.
Gilt $p \equiv 1 \bmod q^2$, so besteht $T\left(\frac{m}{p^k}, q^2\right)$, d.h. jedes dieser Intervallen enthält $\varphi\left(\frac{m}{p^k}\right)/q^2$ Totative. Summation und Multiplikation mit p^k ergibt $\frac{\varphi(p^n)}{q^2}(q-1)$.

Ist $m = p$ und $p \equiv -1 \bmod q^2$, so gilt $E(q^2, 1, p) = E(q^2, 2, p) = \ldots = E(q^2, q^2-2, p) = \mu(p)\mathfrak{P}(p) = -2$, d.h. $p + 1 = q^2$. $\varphi(q^2, i, p)$ für alle $i = 1, \ldots, q^2-2$. Da $q - 1 < q^2 - 2$ $(q \geq 2)$ ergibt sich durch Summieren die Behauptung.

Corollar 92.1 Voraussetzungen wie im vorigen Satz und q = 2. Dann gilt

$$D_{min} \geq p^{n-1} \frac{(p-1)}{4} \quad \text{falls } p \equiv 1 \bmod 4$$

$$D_{min} \geq \frac{p+1}{4} \quad \text{falls } n = 1 \text{ und } p \equiv -1 \bmod 4$$

Ist n = 1, so haben wir eine vollständige Alternative.

Bemerkung Im Spezialfall n = 1 gibt Corollar 92.1 gerade die von Mandelbaum [42] abgeleiteten Schranken.
Ist n > 1, so lässt sich die folgende Aussage ableiten.

Satz 93 Unter denselben Voraussetzungen wie im vorigen Corollar und $p \not\equiv 1 \bmod 4$ gilt

$$D_{min} \geq p^{n-2} \frac{p(p-1)-2}{4} \quad \text{falls } n > 1$$

Beweis $E(4, 1, m/p^k) = \lambda(m/p^k)\,\nu(m/p^k) = 2(-1)^{n-k} = \varphi(p^{n-k}) - 4\varphi(4, 1, p^{n-k})$ und damit

$$p^k\, SB_2\left(\frac{m}{p^k}\right) = \frac{\varphi(p^n) + 2 \cdot (-1)^{n+1-k} p^k}{4}$$

Das Minimum wird bei k = n - 2 angenommen.

Definition 31 Sei $\frac{x}{m} < 1$ ein rationaler Bruch mit (x, m) = 1 und q eine ganze Zahl, so dass $2 \leq q < m$. Gilt dann für gegebenes j und $\varepsilon > 0$

$$|N_q(B_j, m)/\omega_q(m) - 1/q^j| < \varepsilon$$

für jeden Block B_j von j Ziffern der in der Periode der q-nären Darstellung auftritt, so wird x/m als (j, ε) - normal zur Basis q bezeichnet.

Satz 94 (Stoneham [63]) Der rationale Bruch $\frac{x}{p^n} < 1$ (p ungerade Primzahl) mit (x, p) = 1 und $n > z \geq 1$, wo $p^z \| (q^{\omega_q(p)} - 1)$ ist (j, ε) - normal zur Basis q für alle $j \geq \lceil \log_q p^{n-z} \rceil$ und $\varepsilon = 1/p^{n-z}$, wobei $2 \leq q < p^{n-z}$.

Satz 95 Sei $m = p^n$ $(n > 1)$, $mg = q^\lambda - 1$, $\lambda = \omega_q(p^n)$ und $2 \leq [\log_q p]$ sowie -q primitives Element modulo p nicht jedoch q. Weiter gelte $p \| (q^{\omega_q(p)} - 1)$, $4 \leq q^2 < p$ und $g > q$, dann hat man

$$D_{min} \geq \text{Min}\{LB1, LB2\}$$

$$LB1 = \left[(q-1)\left(\frac{1}{q^2} - \frac{1}{p}\right) \cdot \frac{p-1}{2} \cdot p^{n-1} \right]$$

$$LB2 = \frac{1}{2}\left(\left[q\,\frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]\right) \cdot p^{n-1}$$

Es gilt $\omega_q(p) = \frac{p-1}{2}$ und $\omega_q(p^n) = \frac{p-1}{2} \cdot p^{n-1}$.

Beweis Die Aussage $\omega_q(p) = \frac{p-1}{2}$ ist klar, während $\omega_q(p^n) = \frac{p-1}{2}\, p^{n-1}$ aus einem bekannten Satz der Elementaren Zahlentheorie (siehe Le Veque [36] Vol. I p. 52) folgt. Jeder Codepunkte gx lässt sich nun schreiben

$$g \cdot p^{n-k} \cdot x' = \frac{x'}{p^k}(q^\lambda - 1)$$

wenn $(x, p^n) = p^{n-k}$ $(k = 1, \ldots, n)$. Daraus folgt nach dem vorigen Satz

$$N(B_2, p^k) \geq \frac{1}{p^2} - \frac{1}{p^{k-1}}\ \omega_q(p^k)$$

für alle $k \geq 2$. Da wir die Anzahl der Blöcke $\emptyset z$ $(1 \leq z \leq q-1)$ abschätzen, so ergibt sich der Faktor q - 1, weiter muss man noch mit $\lambda/\omega_q(p^k)$ multiplizieren wegen des Faktors $q^\lambda - 1$. Das Minimum über alle $k \geq 2$ genommen ergibt gerade LB1. Es bleibt noch k = 1 übrig, der Fall, der durch den vorigen Satz nicht erfasst wird:

$$g \cdot p^{n-1} \cdot x' = \frac{x'}{p}(q^\lambda - 1)$$

Eine Abschätzung nach unten für das Gewicht dieser Codepunkte erhalten wir aus Satz 110 und Corollar 63.1 Damit ist das Gewicht aller Codepunkte gx nach unten abgeschätzt und wegen Corollar 103.1 ist dies auch eine untere Schranke für D_{min}.

Satz 96 Dieselben Voraussetzungen wie im vorigen Satz aber -q sei nicht notwendig primitives Element modulo p. Dann gilt

$$D_{min} \geq \text{Min}\{LB, DM\}$$

$$LB = \left[(q-1)\left(\frac{1}{q^2} - \frac{1}{p}\right)\cdot\omega_q(p)\cdot p^{n-1}\right]$$

$$DM = p^{n-1}\cdot D_{min}\left[\prod_{q(q^{\omega_q(p)}-1)} \left(\frac{\omega_q(p)}{q^{\omega_q(p)} - 1/p}\right)\right]$$

Beweis Dies ist eine leichte Verallgemeinerung des vorigen Satzes, die man ganz entsprechend beweist.

Bemerkung Satz 96 lässt sich noch weiter verallgemeinern, indem man die Voraussetzung $p \nmid q^{\omega_q(p)} - 1$ streicht. Für wirkliche Berechnungen ist eine solche weitergehende Aussage im allgemeinen nicht mehr zu gebrauchen. Ist $p - 1/\omega_q(p)$ nicht zu gross, so lassen sich mittels Satz 96 praktisch brauchbare untere Schranken für D_{min} ausrechnen.

4.3 Der zyklische GNAF

Definition 32 Sei $m \cdot g = q^l - 1$. Dann teilen wir das Intervall $[0, q^l)$ in drei Teilintervalle:

$$U = \left[\frac{q^{l+1}}{q+1}, q^l\right)$$

$$M = \left[\frac{q^l}{q+1}, \frac{q^{l+1}}{q+1}\right)$$

$$L = \left[0, \frac{q^l}{q+1}\right)$$

Lemma 97 Sei $n \in [0, q^l)$ und $n = (\beta_l, \beta_{l-1}, \ldots, \beta_0)$ die GNAF-Darstellung von n, dann gilt:

(i) $(\beta_l, \beta_{l-1}) = (0, 0) \Longleftrightarrow n \in L$

(ii) $(\beta_l, \beta_{l-1}) = (0, x),\ x > 0 \Longleftrightarrow n \in M$

(iii) $(\beta_l, \beta_{l-1}) = (1, 0) \Longleftrightarrow n \in U$

Beweis Folgt durch genaue Analyse des Verfahrens nach Satz 32.

Lemma 98 Sei $x \in [0, q^l)$, $mg = q^l - 1$.

(i) $x \in U \Longrightarrow mg - x \in L$

(ii) $x \in L \Longrightarrow mg - x \in U$

mit Ausnahme eines Elementes aus L:

a. $2 \mid l$

$x = (0, 0, q-1, 0, q-1, \ldots, 0, q-1)$

b. $2 \nmid l$

$x = (0, 0, q-1, 0, q-1, \ldots, 0, q-1, 0)$

In diesem Fall gilt $mg - x \in M$.

(iii) $x \in M \Longrightarrow mg - x \in M$

mit Ausnahme eines Elementes aus M:

a. $2 \mid l$

$x = (0, q-1, 0, q-1, \ldots, q-1, 0)$

b. $2 \nmid l$

$x = (0, q-1, 0, q-1, \ldots, 0, q-1)$

In diesem Fall gilt $mg - x \in L$.

Die unter a. bzw. b. angegebenen Ausnahmepunkte bestehen aus $l + 1$ Gliedern.

Beweis Ist im wesentlichen klar. Die Ausnahmeelemente erhält man nach Lemma 97 und

a. $x = \frac{q^l - 1}{q + 1} \in L \Longrightarrow mg - x = \frac{q^{l+1} - q}{q + 1} \in M$

bzw.

b. $x = \frac{q^l - q}{q + 1} \in L \Longrightarrow mg - x = \frac{q^{l+1} - 1}{q + 1} \in M$

Im Fall (iii) :

a. $x = \frac{q^{l+1} - q}{q + 1} \in M \Longrightarrow mg - x = \frac{q^l - 1}{q + 1} \in L$

b. $x = \frac{q^{l+1} - 1}{q + 1} \in M \Longrightarrow mg - x = \frac{q^l - q}{q + 1} \in L$

Dabei hat man zu beachten: $q+1 \mid q^i - k \Longleftrightarrow k = \begin{cases} 1 \\ q \end{cases}$ und $2 \mid i$ oder $2 \mid i-1$ $(i > 1)$.

Lemma 99 Sei $mg = q^l - 1 \quad (l > 1)$.

$$x \in L \Longrightarrow \|x\|_q = \|\bar{x}\|_{q(mg)}$$

Beweis Aus Lemma 97 folgt $\|q^l - x\|_q = \|x\|_q + 1$. Weiter gilt

$$\|x\|_q + 1 = \|q^l - x\|_q = \|q^l - 1 - x + 1\|_q \leq \|q^l - 1 - x\|_q + 1$$

und $\|\bar{x}\|_q = \|q^l - 1 - x\|_q = \|mg - x\|_q$

$$\|\bar{x}\|^*_{q(mg)} = \text{Min}\left\{\|x\|_q, \|mg - x\|_q\right\} = \|x\|_q$$

Nach Satz 62 ist aber $\|x\|^*_{q(mg)} = \|\bar{x}\|_{q(mg)}$

Definition 33 Sei $mg = q^l - 1$ $(l > 1)$ und $|n| < mg$. Dann ist der GNAF von n zyklisch, wenn aus der GNAF-Darstellung $n = (\beta_{l-1}, \ldots, \beta_0)$ folgt $n' = (\beta_{l-2}, \ldots, \beta_0, \beta_{l-1})$ ist ebenfalls eine GNAF-Darstellung.

Lemma 100 Alle Elemente aus L besitzen einen zyklischen GNAF.

Lemma 101 Ist $x \in [0, q^l)$, so besitzt x oder $x' = (q^l - 1) - x$ einen zyklischen GNAF.

Beweis 1. $x \in L$, dann besitzt nach dem vorigen Lemma x einen zyklischen GNAF.

2. $x \in U$, dann folgt aus Lemma 98 $x' \in L$ und alles ergibt sich nach a.

3. $x \in M$, dann kann x oder x' einen zyklischen GNAF besitzen. Addieren wir x und x' in GNAF-Darstellung mit eventuell negativem Übertrag, so ist die Summe s gleich $q^l - 1$.

$(|\beta_i| < q) \quad x = (\beta_l, \beta_{l-1}, \ldots, \beta_0) \qquad \beta_l = \beta'_l = 0$

$(|\beta_i'| < q) \quad x' = (\beta'_l, \beta'_{l-1}, \ldots, \beta'_0) \qquad \text{und } \beta_{l-1}, \beta'_{l-1} > 0$

$$s = (\delta_l, \delta_{l-1}, \ldots, \delta_0)$$

Es gibt zwei Möglichkeiten:

(i) $\beta_1 = 1$, $\beta_{1-i} = 0$ $(i = 1, \ldots, l-1)$, $\beta_0 = \overline{1}$ $(\overline{1} = -1!)$

(ii) $\beta_1 = 0$, $\beta_{1-i} = q-1$ $(i = 1, \ldots, l)$

Gilt (ii), so muss notwendig $x = (0, \alpha, \beta, \alpha, \beta, \ldots)$ mit $\alpha + \beta = q-1$ gelten $(\alpha, \beta \geq 0)$. In diesem Fall besitzt x schon einen zyklischen GNAF (wie man sich leicht überlegt besitzen x und x' genau dann einen zyklischen GNAF).
Gilt (i) so ist man gezwungen, eine Reihe von Fallunterscheidungen zu machen. Zuvor überlegt man sich leicht, dass

$$\beta_0 + \beta'_0 = \begin{cases} -1 \\ -q-1 \end{cases} \text{ und } \beta_{l-1} + \beta'_{l-1} = \begin{cases} q \\ q-1 \end{cases}$$

was β_{l-1}, $\beta'_{l-1} \geq 0$ bedeutet. Wir setzen nun voraus x und x' besitzen keinen zyklischen GNAF und betrachten alle möglichen Fälle.

a. $|\beta_{l-1} + \beta_0| \geq q$

Aus $\beta_{l-1} \neq 0$ folgt $\beta_0 \geq 0$ und $\beta_{l-1} + \beta_0 \geq q$, sowie β_{l-1}, $\beta_0 > 0$. Besitzt x' keinen zyklischen GNAF, so unterscheiden wir wieder zwei Fälle.

$|\beta'_{l-1} + \beta'_0| \geq q$: Wir schliessen wie vorhin $\beta'_{l-1} + \beta'_0 \geq q$ mit β'_{l-1}, $\beta'_0 > 0$. Es kann dann nur gelten $\beta_0 + \beta'_0 > 0$, was nicht möglich ist.

$|\beta'_{l-1}| \geq |\beta'_0|$: Eine leichte Folgerung ist $\beta'_{l-1} > 0$, $\beta'_0 < 0$ und $\beta'_{l-1} + \beta'_0 \geq 0$. Nun ist $\beta'_{l-1} = \begin{cases} q-\beta_{l-1} \\ q-1-\beta_{l-1} \end{cases}$ bzw. $\beta'_0 = \begin{cases} -1-\beta_0 \\ -q-1-\beta_0 \end{cases}$

und dies gibt stets einen Widerspruch zu $\beta_{l-1} + \beta_0 \geq q$.

b. $|\beta_{l-1}| \geq |\beta_0|$, d.h. $\beta_{l-1} > 0$ und $\beta_0 < 0$, $\beta_{l-1} + \beta_0 \geq 0$.

$|\beta'_{l-1} + \beta'_0| \geq q$: Ist nicht möglich, dies zeigt man wie vorhin.

$|\beta'_{l-1}| \geq |\beta'_0|$: $\beta'_{l-1} > 0$, $\beta'_0 < 0$, $\beta'_{l-1} + \beta'_0 \geq 0$.

Aus β_0, $\beta'_0 < 0$ ergibt sich $\beta_0 + \beta_0 = -q-1$ und weiter $\beta_{l-1} + \beta'_{l-1} + \beta_0 + \beta'_0 \geq 0$. Also $\beta_{l-1} + \beta'_{l-1} \geq q+1$, ein Widerspruch.

Bemerkung Es gilt genauer : x und x' besitzen genau dann einen zyklischen GNAF, wenn

(i) $x = (0, \alpha, \beta, \alpha, \beta, \ldots, \alpha, \beta), \alpha+\beta = q-1, 2|1$

(ii) $x = (0, \alpha, \alpha, \ldots, \alpha), \alpha = \frac{q-1}{2}, 2 \nmid q, 1$

wobei GNAF-Darstellung und q-adische Darstellung übereinstimmen. Im Fall (i) ist $x' = (0, \beta, \alpha, \beta, \alpha, \ldots, \beta, \alpha)$ und im Fall (ii) gilt $x = x'$ (siehe Clark und Liang [15]).

Satz 102 Sei $x \in [0, q^l)$ und $z = \begin{cases} x, & \text{falls } x \text{ einen zyklischen GNAF hat} \\ x' & \text{sonst} \end{cases}$
mit $x' = q^l - 1 - x$ $(mg = q^l - 1)$. Dann gilt

$$\|\bar{x}\|^*_{q(mg)} = \|z\|_q$$

Besitzen x und x' einen zyklischen GNAF, so ist $\|x\|_q = \|x'\|_q$.

Beweis a. $x \in L$, dann besitzt x einen zyklischen GNAF und aus $\|q^l - x\|_q = 1 + \|x\|_q$ und Lemma 35 (i) folgt $\|x\|_q < \|x'\|_q$.

b. $x \in U$, dann gilt $x' \in L$ und die Behauptung folgt wie unter a.

c. $x \in M$, und wir unterscheiden die Fälle

(i) $q \mid x$

(ii) $q \nmid x$

(i) In diesem Fall besitzt x einen zyklischen GNAF und es gilt $x/_q \in L$ und aus $\|\bar{x}\|^*_{q(mg)} = \|\overline{x/_q}\|^*_{q(mg)}$ (Satz 80) folgt die Behauptung.

(ii) Sei etwa

$$x = (0, \alpha, \beta, \ldots, \gamma, \delta), \alpha > 0$$

Wir zeigen zunächst:

$$\|x\|_q = \|q^l - x\|_q$$

$q^l - x = (0, q-\alpha, \bar{\beta}, \ldots, \bar{\gamma}, \bar{\delta})$ ist wieder eine GNAF-Darstellung mit $0 < q - \alpha$.

$\beta = 0$: klar

$\beta > 0$: $\alpha + \beta < q \Longrightarrow |-\beta| = \beta < q - \alpha$

$\beta < 0$: $-\beta < \alpha \Longrightarrow (q-\alpha) - \beta < q$

Aus Lemma 35 (ii) folgt $\|(q^l - x) - 1\|_q = \|q^l - x\|_q - c$ mit $c = \begin{cases} \emptyset \\ 1 \end{cases}$ $(q \nmid x \Longrightarrow q \nmid q^l - x!)$, d.h. $\|x'\|_q \leq \|x\|_q$.

Besitzt nun x keinen zyklischen GNAF, so ist nach Lemma 101 alles gezeigt. Hat x einen zyklischen GNAF, so muss notwendig gelten $q \nmid x'$ (dies kann man sich leicht überlegen). Dann zeigen unsere Überlegungen aber $\|x'\|_q \leq \|x\|_q$ und $\|x\|_q \leq \|x'\|_q$ $(x'' = x!)$, also $\|x\|_q = \|x'\|_q$. Wir haben bei diesen Überlegungen vorausgesetzt, dass aus $x \in M$ stets $x' \in M$ folgt, dies gilt jedoch nicht für den Ausnahmepunkt. Die Behauptung lässt sich für ihn direkt bestätigen.

Corollar 102.1 Sei $mg = q^l - 1$. Dann gilt

$$D_{min}\left[\|\|_{q(mg)}\ (\overline{g})\right] = \|x\|_q\ ,\ x \in [0,\ q^l)$$

x besitzt einen zyklischen GNAF und ist ein Codepunkt $(x = gy)$.

Beweis Folgt aus dem vorigen Satz, wenn man beachtet, dass mit x auch $x' = mg - x$ Codepunkt ist.

Satz 103 Gilt $m > q$, so existiert ein Codepunkt $x \in L$ mit $\|x\|_q = D_{min}$.

Beweis Wir bestimmen x gemäss Corollar 102.1, ist dann $x \in L$ so sind wir fertig. Da $x \in U$ nicht möglich ist, bleibt noch der Fall $x \in M$. Aus $m > q$ folgt $g = \frac{q^l - 1}{m} < \frac{q^l}{q+1}$, d.h. $g \in L$. Daraus ergibt sich, dass der GNAF von x (ausser der führenden Null) noch eine weitere Null enthalten muss,

$$x = (0, \alpha_{l-1}, \ldots, \alpha_i, \ldots, \alpha_0),\ \alpha_i = 0 \quad (0 \leq i < l-1)$$

denn sonst würde gelten $\|g\|_q < \|x\|_q$. Da x einen zyklischen GNAF besitzt erhalten wir durch zyklischen (links-)shift

$$x_c = (0, \alpha_i, \ldots, \alpha_0, \alpha_{l-1}, \ldots, \alpha_{i-1})$$

und: $x_c \geq 0 \Longrightarrow x_c \in L$

$x_c < 0 \Longrightarrow -x_c \in L$.

Man überlegt sich leicht, dass durch einen solchen shift ein Codepunkt wieder in einen Codepunkt überführt wird. Aus $\|x_c\|_q = \|x\|_q$ folgt die Behauptung.

Corollar 103.1 Sind gx_i $(i = 1, \ldots, N-2)$ die kleinsten positiven Repräsentanten aus den nichttrivialen Orbits von CYL_q und gilt $m > q$, so ist

$$D_{min} = \text{Min} \left\{ \|gx_i\|_q \mid i = 1, \ldots, N-2 \right\}$$

Beweis Dies ist eine Verschärfung von Satz 30 (ii), sie folgt aus Lemma 100 und Satz 102. Denn der Codepunkt $gx \in L$ mit der Eigenschaft $D_{min} = \|gx\|_q$ gehört zu einem Orbit mit dem Repräsentanten gx_j und es gilt $gx_j \leq gx$, da gx_j kleinster Repräsentant ist. Daraus folgt $gx_j \in L$ und nach Lemma 100 und Satz 102 $\|gx_j\|_q = \|\overline{gx_j}\|^* = \|\overline{gx}\|^* = \|gx\|_q = D_{min}$.

Satz 104 Sei $mg = q^l - 1$ $(l > 1)$ und $x \in [0, q^l)$. Besitzt x einen zyklischen GNAF, so ist $\|x\|_q \,(= \|\bar{x}\|^*_{q(mg)})$ gleich der Anzahl der Reste $R_{mg}(q^i x)$ $(i = 0, 1, \ldots, l-1)$ welche im Intervall M liegen.

Beweis Sei $x = (0, \alpha_{l-1}, \ldots, \alpha_0)$ die GNAF-Darstellung und $x_i = (0, \alpha_{l-1-i}, \ldots, \alpha_0, \alpha_{l-1}, \ldots, \alpha_{l-i})$ $(0 < i \leq l-1)$, $x_0 = x$ durch zyklischen Shift aus x entstanden. Dann ist klar

$$x_i = \begin{cases} R_{mg}(q^i x) & \text{falls } x_i \geq 0 \\ R_{mg}(q^i x) - mg & \text{falls } x_i < 0 \end{cases}$$

Es gilt nun weiterhin

$$\alpha_{l-1-i} > 0 \Longleftrightarrow R_{mg}(q^i x) = x_i \in M$$

$$\alpha_{l-1-i} < 0 \Longleftrightarrow mg - R_{mg}(q^i x) = -x_i \in M$$

Daraus folgt,

$$\alpha_{l-1-i} \neq 0 \Longleftrightarrow R_{mg}(q^i x) \in M$$

wie leicht mit Lemma 97 und 98 nachzuweisen ist.

Corollar 104.1 Sei $mg = q^l - 1$ $(l > 1)$ und $g > q$. Ist gx ein Codepunkt $(0 < x < m)$ mit zyklischem GNAF, so ist $\|\overline{gx}\|^*_{q(mg)}$ gleich der Anzahl der Reste $R_m(q^i x)$ $(i = 0, 1, \ldots, l-1)$ welche im Intervall $M_g = (m/q+1,\ q \cdot m/q+1]$ liegen.

Beweis Aus dem vorigen Satz wissen wir bereits, dass $\|gx\|^*_{q(mg)}$ gleich der Anzahl der Reste $R_{mg}(q^i gx) \in M$ ist.

Nun ist $R_{mg}(q^i gx) = g\, R_m(q^i x)$ und

$$g \cdot R_m(q^i x) \in M \Longleftrightarrow g \cdot m + 1 \leq (q+1) \cdot g \cdot R_m(q^i x) < q \cdot (gm + 1)$$

wenn man $g \cdot m = q^l - 1$ beachtet. Weiter gilt

$$gm + 1 \leq (q+1) \cdot g \cdot R_m(q^i x) \Longleftrightarrow gm < (q+1) \cdot g \cdot R_m(q^i x)$$

und

$$(q+1) \cdot g \cdot R_m(q^i x) < q \cdot gm + q \Longleftrightarrow (q+1) \cdot g \cdot R_m(q^i x) \leq q \cdot gm$$

denn unter der Voraussetzung $g > q$ kann niemals $(q+1) \cdot g \cdot R_m(q^i x) = q \cdot g \cdot m + q - k$ für ein $0 \leq k \leq q-1$ gelten.

Satz 105 Sei $mg = q^l - 1$ und $m > q$. Dann ist das Gewicht eines Codepunktes $gx \in L$ gleich der Anzahl der Reste $R_m(q^i x)$ $(i = 1, \ldots, l)$ die im Intervall M_g liegen.

Beweis Aus $gx \in L$ folgt $g(q+1)x \in [0, q^l)$ und damit gilt, wenn

$$gx = (\alpha_{l-1}, \ldots, \alpha_0)$$
$$g(q+1)x = (\beta_{l-1}, \ldots, \beta_0)$$

die q-nären Darstellungen sind, nach Lemma 78

$$(i = 1, \ldots, l)\quad \alpha_{l-i} = R_q(R_{mg}(q^i xg)) = R_q(g \cdot R_m(q^i x))\quad (0 \leq x < m)$$
$$\beta_{l-i} = R_q(R_{mg}(q^i (q+1) xg)) = R_q(g \cdot R_m(q^i (q+1) x))$$

Nun gilt nach Satz 32 für die GNAF-Darstellung

$$qgx = \sum_{i=1}^{l} (\beta_{l-i} - \alpha_{l-i})\, q^{l-i}$$

Um Das Gewicht von qgx und damit auch von gx zu bestimmen müssen wir demnach feststellen wie oft $\alpha_{l-i} \neq \beta_{l-i}$ gilt.

Sei nun $R_m(q^i x) \in M_g$.

$$R_m(q^i x) \in M_g \iff m < (q+1)\, R_m(xq^i) \leq q \cdot m$$

Es gilt $R_m((q+1)\, xq^i) = R_m((q+1)\, R_m(xq^i))$, also

$$R_m((q+1)xq^i) = (q+1)\, R_m(xq^i) - c \cdot m \quad (1 \leq c \leq q)$$

Wir untersuchen den Fall $R_m((q+1)xq^i) = 0$, d.h. $(q+1)\, R_m(xq^i) = c \cdot m$. Es genügt zu untersuchen ob eventuell gelten kann $R_m(xq^i) = k \cdot q$ $(k > 0)$. Würde das wahr sein, so $(q+1) \cdot k \cdot q = c \cdot m$ und wegen $(q,m) = 1$ bedeutet es $k' \cdot q = c$, also $k' = 1$ und $c = q$ ($R_m(xq^i) = 0$ ist wegen $c > 0$ nicht möglich!). Nun kann $c = q$ nur gelten, wenn $q+1 \mid m$ ist, also

$$(q+1) \cdot k \cdot q = q \cdot \frac{m}{q+1} \cdot (q+1) \quad \text{und} \quad k = \frac{m}{q+1}$$

Das bedeutet,

$$x \cdot q^i \equiv \frac{m}{q+1} \cdot q \bmod m$$

somit $\frac{m}{q+1} \mid x \cdot q^i$ und wegen $(q, m) = 1$ gilt $\frac{m}{q+1} \mid x$. Da nach Voraussetzung $gx \in L$, so muss $g \cdot \frac{m}{q+1} \cdot a < \frac{gm+1}{q+1}$, d. h. $a = 1$ und $x = \frac{m}{q+1}$. Wir haben dann $gx = \frac{gm}{q+1} = \frac{q^l - 1}{q+1}$ und $(q+1)\, gx = gm = q^l - 1$. Es liegt der in Lemma 98 unter (ii) a. als Ausnahmepunkt behandelte Fall vor. Insbesondere ist dann auch der Ausdruck für β_{l-i} nicht mehr gültig. Es ist dann,

$$R_m\left(\frac{m}{q+1} \cdot q^i\right) = \frac{m}{q+1} \quad R_{q+1}(q^i)$$

und da $R_{q+1}(q^i)$ entweder 1 oder q ist je nachdem $2 \mid i$ oder $2 \nmid i$, so ist $R_m\left(\frac{m}{q+1} \cdot q^i\right)$ abwechselnd gleich $\frac{m}{q+1}$ oder $q \cdot \frac{m}{q+1}$, d.h. das Gewicht von $\frac{q^l - 1}{q+1}$ $(2 \mid l!)$ ist 1/2 und gleich der Anzahl der Reste $R_m\left(\frac{m}{q+1} \cdot q^i\right)$ im Intervall M_g.

Es bleibt noch übrig $R_m((q+1)\, xq^i) = (q+1)\, R_m(xq^i) - c \cdot m$ mit $1 \leq c < q$ zu untersuchen. Man sieht leicht ein, dass in diesem Fall $\alpha_{l-i} \neq \beta_{l-i}$ gilt.

Sei nun $R_m(q^i x) \notin M_g$, d.h.

$$q \cdot m < (q+1)\, R_m(xq^i) < (q+1)\, m$$

oder $0 \leq (q+1)\, R_m(xq^i) < m$

Man überlegt sich leicht, dass in beiden Fällen $\alpha_{l-i} = \beta_{l-i}$ gilt (eine Ausnahme ist wieder $(q+1)\, R_m(xq^i) = m$, siehe oben).

Bemerkung Es dürfte klar sein, dass man den Exponenten i in $R_m(xq^i)$ statt von 1 bis l auch von 0 bis l-1 laufen lassen kann.

Satz 106 Sei $mg = q^l - 1$ $(l > 1)$ und $g > q$. Dann gilt

$$D_{min} = \min_{0<x<m} \left\{ \left| Z(x) \cap M_g \right| \cdot 1/\omega_q(m/d) \right\} \qquad (d = (x, m))$$

$$= \min_{d|m} \left\{ \min_{(x,m)=d} \left\{ \left| Z(x) \cap M_g \right| \right\} \cdot \frac{1}{\omega_q(m/d)} \right\}$$

Beweis Besitzt gx einen zyklischen GNAF, so ist $\|\overline{gx}\|^*_{q(mg)}$ gleich $|Z(x) \cap M_g| \cdot 1/\omega_q(m/d)$ nach Corollar 104.1. Hat gx keinen zyklischen GNAF, so nach Lemma 101 $gx' = mg - gx = g(m-x)$. Wir zeigen nun

$$|Z(x) \cap M_g| = |Z(x') \cap M_g| \qquad (x' = m - x)$$

Es gilt $R_m(x'q^i) = m - R_m(xq^i)$ und

$(m - R_m(xq^i) = \frac{m}{q+1}$ oder $m - R_m(xq^i) \in M_g) \Longleftrightarrow (R_m(xq^i) \in M_g$ oder $R_m(xq^i) = \frac{m}{q+1})$

Aus $R_m(xq^i) = \frac{m}{q+1}$ folgt aber $R_m(x\, q^{i+1}) = q \cdot \frac{m}{q+1}$ und wegen $R_m(xq^i) = \frac{m}{q+1} \Longleftrightarrow m - R_m(xq^i) = q\,\frac{m}{q+1}$ ist alles gezeigt.

Bemerkung Statt das Minimum über alle $0 < x < m$ zu nehmen wird man natürlich nur ein Repräsentantensystem aller zyklischen Klassen Z(x) nehmen. Das ist gleichbedeutend mit einem System x_i (i = 1, ..., N-2) von Repräsentanten gx_i der nichttrivialen Orbits von $Z(CYL_q)$ (siehe Corollar 103.1).

Corollar 106.1 Sei $0 < x < m$. Dann gilt

$$|Z(x) \cap M_g| = |Z(x') \cap M_g| \qquad (x' = m - x)$$

Bemerkung

a. In Satz 104 und Corollar 104.1 ist zu beachten, dass wir die Folge der Reste $R_{mg}(q^i x)$ bzw. $R_m(q^i x)$ betrachten. Es werden deshalb eventuell gleiche Reste, aber mit verschiedenem Index i, mehrfach gezählt.

b. In der Theorie der zyklischen Codes ist Satz 106 von zentraler Bedeutung. Mit seiner Hilfe gelingt es unter speziellen Voraussetzungen D_{min} exakt zu bestimmen oder untere bzw. obere Schranken für D_{min} abzuleiten.

c. Im Fall $q = 2$ ist alles was wir oben gezeigt haben schon längere Zeit bekannt, siehe den Übersichtsartikel von Massey/Garcia [44]. Die entsprechenden Techniken wurden vor allem von Goto und Fukumura [23], Chien et al. [12] und Preparata [51] entwickelt. Die Verallgemeinerung auf $q > 2$ wird in einer Arbeit von Clark und Liang [15] z.T. ohne Beweise skizziert. Wir gehen in unserer Darstellung einen etwas anderen Weg und erreichen dadurch eine gewisse Vereinfachung.

d. Die ersten Ansätze zu den oben benutzten Techniken findet man in der Dissertation von Tsao-Wu [66]. Insbesondere gehen (indirekt) Satz 105 und Satz 106 auf ihn zurück. Er benutzt die durch Satz 106 nahegelegte Technik um D_{min} (alles für $q = 2$!) zu bestimmen. Der Beweis des entsprechenden Satzes ist jedoch falsch.

Lemma 107 Sei $g \cdot m = q^l - 1 = g' \cdot m'$ $(l > 1)$, $g, g' > q$ und $m' \mid m$. Dann gilt

$$D_{min}\left[\| \|_{q(mg)}(\overline{g})\right] \leq D_{min}\left[\| \|_{q(m'g')}(\overline{g'})\right]$$

Beweis Ist $m = m'$ so ist alles klar. Gilt $m' < m$, so folgt aus $d' \mid m'$, $d \mid m$ wo $d = d' \cdot \frac{m}{m'}$. Sei $g'x$ ein Codepunkt mit $(x, m') = d'$ und $x/d' = x'$, dann ist $gx'd$ ein Codepunkt mit $(x'd, m) = d$.

$R_m\ (q^i x' d) \in M_g$ ist äquivalent zu $R_m, (q^i x) \in M_g \,/\, \frac{m}{m'} = M_{g'}$.
Zusammen mit Satz 106 folgt die Behauptung
$(M_g/n = \left(\frac{m}{(q+1)n}\ ,\ q \cdot \frac{m}{(q+1)\cdot n}\right])$.

Lemma 108 Sei $g \cdot m = q^l - 1$ $(l > 1)$, $m > q$ und der Code kann alle t-fachen Fehler korrigieren, d.h. $D_{min} \geq 2\,t + 1$ $(t > 0)$. Ist der Code dann perfekt, so gilt $D_{min} = 2\,t + 1$.

Beweis Nach Satz 103 existiert ein Codepunkt $x \in L$ mit $\|x\|_q = D_{min}$. Sei $x = \sum_{i=0}^{l} \alpha_i q^i$ der GNAF von x, wobei nach Lemma 97 (i) $\alpha_l = \alpha_{l-1} = 0$ gilt. Dann existiert ein $0 < c < l$ mit der Eigenschaft

$$x' = \sum_{i=c}^{l} \alpha_i q^i > 0 \quad , \quad \|x'\|_q = t + 1 \text{ und } x' \in L.$$

Da der Code perfekt ist muss ein Codepunkt $\bar{r}$ existieren, so dass $\overline{x'} \in B\ (\bar{r},\ t)$ gilt. Aus $D_{min} > 2\ t+1$ folgt $\|\bar{r}\|^*_{q(mg)} > 2\ t+1$ und

$\|\bar{r}\|^*_{q(mg)} = \|\bar{r} - \overline{x'} + \overline{x'}\|^*_{q(mg)} \leq \|\bar{r} - \overline{x'}\|^*_{q(mg)} + \|\bar{x}\|^*_{q(mg)} \leq 2\ t+1$,

da nach Lemma 100 und Satz 102 $\|x'\|_q = \|\bar{x}'\|^*_{q(mg)} = t+1$ gilt und $\|\bar{r} - \overline{x'}\|^*_{q(mg)} \leq t$ aus $\overline{x'} \in B\ (\bar{r},\ t)$ folgt. Demnach muss $D_{min} = 2\ t + 1$ gelten.

4.4 Die Berechnung von D_{min} für spezielle Werte von m

Unsere bisherigen Untersuchungen lassen sich wie folgt zusammenfassen: Die Zahlen gx im Intervall $[0,\ q^l - 1]$ $(mg = q^l - 1,\ l > 1)$ lassen sich bezüglich der Basis q in Klassen disjunkter Orbits zerlegen. Die Zahlen eines Orbits gehen durch zyklische Linksshifts ihrer q-nären Darstellungen ineinander über und dies ist zugleich die Definition eines Orbits. Jedem Orbit entspricht umkehrbar eindeutig eine zyklische Klasse Z(x) von Resten modulo m. Die zyklischen Klassen bilden eine Partition der Reste modulo m. Alle Elemente eines Orbits besitzen das gleiche modulare Gewicht.

Um D_{min} zu bestimmen genügt es Repräsentanten für alle zyklischen Klassen zu kennen, und damit besitzen wir zugleich Repräsentanten für sämtliche Orbits. Unter der Voraussetzung $g > q$ lässt sich D_{min} dann nach Satz 106 durch Abzählen der Elemente der zyklischen Klassen, welche im Intervall M_g liegen, bestimmen. Hat man kleinste Repräsentanten und gilt $m > q$, so kann man D_{min} nach Corollar 103.1 finden, wenn es gelingt, das Gewicht aller Repräsentanten zu bestimmen. Es ist klar wie entsprechend modifizierte Überlegungen zu oberen oder unteren Schranken für D_{min} führen.
Wir untersuchen zunächst den Fall $m = p$ (ungerade Primzahl). Um Repräsentanten für die zyklischen Klassen zu erhalten, benutzen wir das folgende Lemma, welches aus einer elementaren Aussage über die Untergruppen endlicher zyklischer Gruppen folgt.

Lemma 109 Sei ς primitive Wurzel modulo m. Dann ist $1 = \varsigma^0, \varsigma^1, \ldots, \varsigma^{s-1}$ mit $s = \varphi(m)/\omega_q(m)$ ein Repräsentantensystem der Nebenklassen, der von q ($(q, m) = 1$) erzeugten Untergruppe.

Bemerkung Es muss gelten $m = p^\alpha$ oder $m = 2\,p^\alpha$ ($p > 2$, Primzahl), da sonst keine primitive Wurzel existiert. Wir schränken zunächst auf $\alpha = 1$ ein.

Satz 110 Sei $m = p$ eine ungerade Primzahl und q primitive Wurzel modulo p, weiter gelte $gp = q^{p-1} - 1$. Unter der Voraussetzung $g > q$ gilt,

$$D_{min} = \left[q \frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]$$

und der Code ist äqudistant.

Beweis Kleinster Repräsentant der einzigen zyklischen Klasse ist 1. Aus Satz 106 folgt sofort die Behauptung. Der Code ist äquidistant nach Satz 80.

Corollar 110.1 Unter den gleichen Voraussetzungen wie im vorigen Satz gilt:

(i) $p \equiv 1 \bmod q + 1 \longrightarrow D_{min} = (q-1)\ \frac{p-1}{q+1}$

(ii) $p \equiv -1 \bmod q+1 \longrightarrow D_{min} = (q-1)\ \frac{p+1}{q+1}$

(iii) $p = q + 1 \Longrightarrow D_{min} = q - 1$

Beweis Dies folgt direkt aus dem vorigen Satz.

Bemerkung

a. Man beachte, dass für $q = 2$ Corollar 110.1 eine vollständige Alternative darstellt. Aus $p \equiv 1 \bmod 3$ folgt $D_{min} = \frac{p-1}{3}$, aus $p \equiv -1 \bmod 3$ folgt $D_{min} = \frac{p+1}{3}$ und aus $p = 3$ folgt $D_{min} = 1$.

b. Satz 110 wurde für $q = 2$ von Barrows [3], allerdings mit wesentlich komplizierteren Methoden abgeleitet, während Mandelbaum [42], unabhängig von Barrows, obere und untere Schranken bestimmte. Die Verallgemeinerung für Werte $q > 2$ rührt von Clark und Liang [15] her.

Satz 111 Sei $m = p$ eine ungerade Primzahl und q primitive Wurzel modulo p nicht jedoch q. Ist $g \cdot p = q^{\frac{p-1}{2}} - 1$ und $g > q$, so gilt

$$D_{min} = \frac{1}{2}\left(\left[q\,\frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]\right)$$

und der Code ist äquidistant.

Beweis Aus der Voraussetzung folgt $\omega_q(p) = \frac{p-1}{2}$ und nach Lemma 109 sind 1 und - 1 Repräsentanten der beiden Nebenklassen:

$$Z(1) = \{1, q, \ldots, q^{\frac{p-1}{2}} - 1\}$$

$$Z(-1) = \{-1, -q, \ldots, -q^{\frac{p-1}{2}} - 1\}$$

Aus Satz 106 und Corollar 106.1 folgt die Behauptung. Der Code ist äquidistant weil die Elemente der beiden Orbits nach Corollar 106.1

das gleiche Gewicht besitzen.

Corollar 111.1 Unter den gleichen Voraussetzungen wie im vorigen Satz gilt:

(i) $p \equiv 1 \bmod q+1 \Longrightarrow D_{min} = \frac{1}{2}(q-1)\frac{p-1}{q+1}$

(ii) $p \equiv -1 \bmod q+1 \Longrightarrow D_{min} = \frac{1}{2}(q-1)\frac{p+1}{q+1}$

Satz 112 Sei $m = p^n$ $(n>1)$, p ungerade Primzahl und q primitive Wurzel modulo p^2. Ist $g \cdot p^n = q^\lambda - 1$, $\lambda = \varphi(p^n) = p^{n-1}(p-1)$ und $g > q$, so gilt

$$D_{min}\left[\|\|_{q(mg)}(\bar{g})\right] = \operatorname{Min}\left\{ p^k \cdot S\left(\frac{m}{p^k}\right) \;\middle|\; k = 0, \ldots, n-1 \right\}$$

$$S\left(\frac{m}{p^k}\right) = \left[q \cdot \frac{m}{p^k(q+1)}\right] - \left[\frac{m}{p^k(q+1)}\right] - \left\{\left[q \cdot \frac{m}{p^k \cdot p(q+1)}\right] - \left[\frac{m}{p^k \cdot p(q+1)}\right]\right\}$$

Beweis Kleinste Repräsentanten der Orbits sind die Codepunkte gp^k $(k = 0, \ldots, n-1)$. Nach Satz 106 müssen wir $|Z(p^k) \cap M_g|$ bestimmen, nun gilt aber

$$R_m(q^i p^k) \in M_g \Longleftrightarrow R_{\frac{m}{p^k}}(q^i) \in M_g/p^k = \left(\frac{m}{p^k(q+1)}, q \cdot \frac{m}{p^k(q+1)}\right]$$

Da q auch primitives Element modulo $\frac{m}{p^k}$ ist müssen wir alle $x \in M_g/p^k$ mit $(x, m/p^k) = 1$, d.h. mit $(x, p) = 1$ bestimmen. Wie man sich leicht überlegt ist $S\left(\frac{m}{p^k}\right)$ gerade gleich dieser Zahl. Der Faktor $1/\omega_q(m/d)$ in Satz 106 ist aber gleich

$$\frac{p^{n-1}(p-1)}{p^{n-k-1}(p-1)} = p^k$$

und alles ist gezeigt.

Satz 113 Unter denselben Voraussetzungen wie im vorigen Satz gilt:

(i) $p = q+1 \Longrightarrow D_{min} = (q-1)\ \frac{\varphi(p^n)}{q+1}$

(ii) $q+1 < p$ und $p \equiv 1 \bmod q+1 \Longrightarrow D_{min} = (q-1)\ \frac{\varphi(p^n)}{q+1}$

und der Code ist äquidistant.

(iii) $q+1 < p$ und $p \equiv -1 \bmod q+1 \Longrightarrow D_{min} = (q-1) \cdot \frac{\varphi(p^n) - 2\,p^{n-2}}{q+1}$

Beweis Aus dem Beweis von Satz 112 entnimmt man, dass $S\left(\frac{m}{p^k}\right)$ gleich der Anzahl der Totative von $\frac{m}{p^k} = p^{n-k}$ im Intervall

$\left(\frac{m}{p^k(q+1)}, q \cdot \frac{m}{p^k(q+1)}\right]$ ist. Gilt $p > q+1$, so ist $j \cdot \frac{m}{p^k(q+1)}$

$(0 < j < q+1)$ niemals Totativ von $\frac{m}{p^k}$.

(i) Folgt durch direktes Auswerten der Formel $S\left(\frac{m}{p^k}\right)$ aus Satz 112.

(ii) Es gilt $T\left(\frac{m}{p^k}, q+1\right)$ für alle $k = 0, \ldots, n-1$, so dass sich ergibt $p^k \cdot S\left(\frac{m}{p^k}\right) = (q-1)\ \frac{\varphi(p^n)}{q+1}$

Äquidistant ist dieser Code, weil alle Orbits das gleiche modulare Gewicht haben.

(iii) Dies folgt leicht durch direktes Auswerten der Formel für $S\left(\frac{m}{p^k}\right)$, wenn man berücksichtigt, dass aus $p \equiv -1 \bmod q+1$ folgt $p^{n-k} \equiv (-1)^{n-k} \bmod q+1$ und die Fälle $n-k$ gerade bzw. $n-k$ ungerade berücksichtigt.

Corollar 113.1 Die Voraussetzungen wie in Satz 112, $q = 2$ und $3 < p$, dann gilt

$$D_{min} = p^{n-2}\ \frac{p(p-1) - \xi(p)}{3}$$

mit

$$\varepsilon(p) = \begin{cases} 0 & \text{falls } p \not\equiv 2 \bmod 3 \\ 2 & \text{sonst} \end{cases}$$

Beweis Wir müssen die Fälle $p \equiv 0 \bmod 3$, $p \equiv 1 \bmod 3$ und $p \equiv 2 \bmod 3$ unterscheiden. Die beiden Ersten sind durch Satz 113 erledigt. Es gilt nun für $p \equiv 2 \bmod 3$ $E(3, 0, p^{n-k}) = -\frac{1}{2}(-1)^{n-k} \cdot 2$ und $E(3, 1, p^{n-k}) = -2E(3, 0, p^{n-k}) = 2 \cdot (-1)^{n-k}$. Daraus folgt

$$\gamma(3, 1, p^{n-k}) = \frac{\varphi(p^{n-k}) - 2 \cdot (-1)^{n-k}}{3} = S\left(\frac{m}{p^k}\right)$$

$$p^k \cdot S\left(\frac{m}{p^k}\right) = \frac{\varphi(p^n) - 2(-1)^{n-k} \cdot p^k}{3}$$

Das Minimum wird bei $k = n - 2$ angenommen.

Corollar 113.2 Voraussetzungen wie im vorigen Corollar, aber $q = 3$.

$$D_{min} = p^{n-2} \frac{p(p-1) - \varepsilon(p)}{2}$$

$$\varepsilon(p) = \begin{cases} 0 & p \not\equiv 3 \bmod 4 \\ 2 & \text{sonst} \end{cases}$$

Beweis Es gilt $E(4, 1, p^{n-k}) = E(4, 2, p^{n-k})$ und $E(4, 1, p^{n-k}) = -E(4, 0, p^{n-k})$. Nun ist aber $E(4, 0, p^{n-k}) = -(-1)^{n-k} \cdot 2$ falls $p \equiv 3 \bmod 4$ gilt. Die Rechnung verläuft wie im vorigen Corollar.

Um geschlossene Ausdrücke für D_{min} zu bestimmen, genügt es jeweils $E(q+1, j, p^{n-k})$ für $j = 1, \ldots, q-1$ zu kennen. Die Berechnung wird mit wachsendem q jedoch immer schwieriger.

Satz 114 Sei $m = p^n$ $(n > 1)$ (p ungerade Primzahl) und $-q$ primitive Wurzel modulo p^2, q sei nicht primitive Wurzel modulo p. Ist $g \cdot p^n = q^{\lambda/2} - 1$, $\lambda = \varphi(p^n) = p^{n-1}(p-1)$ und $g > q$, so gilt

$$D_{min}\left[\| \|_{q(mg)}(\bar{g})\right] = \operatorname{Min}\left\{ \frac{1}{2} p^k S\left(\frac{m}{p^k}\right) \;\middle|\; k = 0, \ldots, n-1 \right\}$$

Beweis Aus der Voraussetzung folgt $\omega_q(p^i) = \frac{\varphi(p^i)}{2}$ für alle $i \geq 1$.

Ein Repräsentantensystem für die Orbits sind gp^k und $gp^k(p^{n-k}-1)$ $(k = 0, \ldots, n-1)$, denn es gilt $\varphi\left(\frac{m}{p^k}\right) / \varphi_q\left(\frac{m}{p^k}\right) = 2$ und da $-q$ primitive Wurzel ist, muss $m - p^k$ Repräsentant des zweiten Orbits sein, d.h. es gibt genau zwei Orbits zu welchen die Codepunkte gx mit $(x, m) = p^k$ gehören. Aus Satz 106 und Corollar 106.1 folgt leicht die Behauptung.

Aus diesem Satz ergibt sich sofort, dass sämtliche Folgerungen, die wir aus Satz 113 gezogen haben, auch in diesem Fall gelten, wenn wir die Werte für D_{min} mit dem Faktor $1/2$ multiplizieren.

Bemerkung

a. Alles was wir ab Satz 110 gezeigt haben, wurde für $q = 2$ von Tsao-Wu in seiner Dissertation [66] abgeleitet. Allerdings sind die Beweise recht lang.
b. Dass die in Satz 110 und Satz 111 angegebenen Codes äquidistant sind, haben zuerst (wieder nur für $q = 2$) Massey und Garcia [44] erkannt. Implizit findet sich dies jedoch schon bei Tsao-Wu [66]. Von Massey/Garcia [44] wird die Vermutung ausgesprochen, dass es die einzigen äquidistanten Codes sind. Wie Satz 113 und Satz 114 zeigen, ist diese Vermutung falsch.
c. Corollar 113.1 und Corollar 113.2 sind natürlich direkte Folgerungen aus Satz 113, der für $q = 2, 3, 5$ eine vollständige Fallunterscheidung liefert. In allen anderen Fällen muss man jedoch die in den beiden Corollaren angegebene Beweistechnik heranziehen.

Satz 115 Sei $m = 2p$ $(p > 2$, Primzahl) und q primitive Wurzel modulo m. Ist $g \cdot 2p = q^\lambda - 1$, $\lambda = \varphi(2p) = p-1$ und $g > q$, so gilt

$$D_{min} = \left[q \frac{2p}{q+1}\right] - \left[\frac{2p}{q+1}\right] - \left\{\left[q \frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]\right\} - 1$$

Beweis Repräsentanten der verschiedenen möglichen Orbits sind

$g \cdot 1$, $g \cdot 2$, $g \cdot p$. Wir bestimmen wieder $|Z(x) \cap M_g|$ $(x = 1, 2, p)$, was ergibt

$$|Z(1) \cap M_g| = \left[q \frac{2p}{q+1}\right] - \left[\frac{2p}{q+1}\right] - \left\{\left[q \frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]\right\} - 1$$

$$|Z(2) \cap M_g| = \left[q \frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right]$$

$$|Z(p) \cap M_g| = 1$$

Der Faktor $\lambda/\omega_q(m/d)$ bestimmt sich für $Z(1)$, $Z(2)$ zu 1 und bei $Z(p)$ zu $p-1$. Benutzen wir die Ungleichung,

$$[x] + [y] \leq [x + y] \leq [x] + [y] + 1$$

welche für reelle x, y gilt, so findet man

$$|Z(1) \cap M_g| \leq \left[q \frac{p}{q+1}\right] + \left[q \frac{p}{q+1}\right] + 1 - \left[\frac{2p}{q+1}\right] - \ldots\ldots$$

$$\leq 2\left[q \frac{p}{q+1}\right] + 1 - 2\left[\frac{p}{q+1}\right] - \left[q \frac{p}{q+1}\right] + \left[\frac{p}{q+1}\right] - 1$$

$$= \left[q \frac{p}{q+1}\right] - \left[\frac{p}{q+1}\right] = |Z(2) \cap M_g|$$

woraus schon alles folgt, wenn man beachtet $|Z(2) \cap M_g| \leq p - 1$.

Bemerkung

a. Man beachte, dass wegen $(2p, q) = 1$ der binäre Fall $q = 2$ ausgeschlossen ist.

b. Zur Illustration kann das Beispiel $3^4 - 1 = 80 = (2 \cdot 5) \cdot 8$ $(m = 2 \cdot 5, g = 8)$ dienen. Da 3 primitive Wurzel modulo 5 ist und zugleich ungerade ist, so muss 3 auch primitive Wurzel modulo 10 sein. Die Orbitstruktur:

$d = 1$

ØØ22	$1 \cdot 8$	$\varphi(2 \cdot 5) = 4$, $\omega_3(2 \cdot 5) = 4$
Ø22Ø	$3 \cdot 8$	
22ØØ	$9 \cdot 8$	
2ØØ2	$7 \cdot 8$	
ØØ22	$1 \cdot 8$	

$d = 2$

Ø121	$2 \cdot 8$	$\varphi(2 \cdot 5/2) = 4$, $\omega_3(2 \cdot 5/2) = 4$
121Ø	$6 \cdot 8$	
21Ø1	$8 \cdot 8$	
1Ø12	$4 \cdot 8$	
Ø121	$2 \quad 8$	

$d = 5 \quad \{1111 \quad 5 \cdot 8 \qquad \vartheta(2 \cdot 5/5) = 1, \quad \omega_3(2 \cdot 5/5) = 1$

$d = 2 \cdot 5 \quad \{2222 \quad (2 \cdot 5) \cdot 8$

$$D_{min} = \left[\frac{30}{4}\right] - \left[\frac{10}{4}\right] - \left\{\left[\frac{15}{4}\right] - \left[\frac{5}{4}\right]\right\} - 1 = 2$$

Durch Inspektion der Orbits bestätigt man den Wert für D_{min} direkt.

c. Gilt $2p > q + 1$, so ist der Wert für D_{min} gleich der Anzahl der Totative von $2p$ im Intervall $\left(\frac{2p}{q+1}, q\,\frac{2p}{q+1}\right)$.

Corollar 115.1 Voraussetzungen wie im vorigen Satz.

(i) $p \equiv 1 \bmod q + 1 \Longrightarrow D_{min} = (q-1)\,\frac{p-1}{q+1}$

und der Code ist f-äquidistant.

(ii) $p \equiv -1 \bmod q + 1 \Longrightarrow D_{min} = (q-1)\,\frac{p+1}{q+1} - 2$

(iii) $p = q + 1 \Longrightarrow D_{min} = q - 2$

Satz 116 Sei $m = 2p^n$ $(n > 1)$, p Primzahl und q primitive Wurzel modulo $2p^n$. Ist $g \cdot 2p^n = q^\lambda - 1$, $\lambda = \vartheta(2p^n) = \vartheta(p^n) = p^{n-1}(p-1)$ und $g > q$, so gilt

$$D_{min} = \text{Min}\left\{ c_{s,k} \cdot S2\left(\frac{m}{2^s p^k}\right) \,\middle|\, k = 0, \ldots, n;\ s = 0,1 \text{ und } s = 0 \text{ wenn } k = n \right\}$$

mit $c_{s,k} = p^k$ ausser, wenn $s = 0$, $k = n$, wo $c_{s,k} = \vartheta(p^n)$ gilt.

$$S2\left(\frac{m}{2p^k}\right) = \left[q \cdot \frac{m}{2p^k(q+1)}\right] - \left[\frac{m}{2p^k(q+1)}\right] - \left\{\left[q \cdot \frac{m}{2p^k \cdot p\,(q+1)}\right] - \left[\frac{m}{2p^k \cdot p\,(q+1)}\right]\right\}$$

$$S2\left(\frac{m}{p^k}\right) = \left[q \cdot \frac{m}{p^k(q+1)}\right] - \left[\frac{m}{p^k(q+1)}\right] - \left\{\left[q \cdot \frac{m}{2p^k(q+1)}\right] - \left[\frac{m}{2p^k(q+1)}\right]\right\} - \left\{\left[q \cdot \frac{m}{p^k \cdot p\,(q+1)}\right] - \left[\frac{m}{p^k \cdot p\,(q+1)}\right]\right\} + \left\{\left[q \cdot \frac{m}{2p^k \cdot p\,(q+1)}\right] - \left[\frac{m}{2p^k \cdot p\,(q+1)}\right]\right\}$$

Beweis Die Überlegungen sind ganz ähnlich wie im Beweis von Satz 113. Wir müssen alle $x \in M_g / 2^s p^k$ mit $(x, m/2^s p^k) = 1$ bestimmen, das sind für $s = 1$ alle x mit $(x, p) = 1$, für $s = 0$ alle x, die noch zusätzlich $(2, x) = 1$ erfüllen. $S2\left(\frac{m}{2p^k}\right)$ $(k = 0, \ldots n-1)$ und $S2\left(\frac{m}{p^k}\right)$ $(k = 0, \ldots, n)$ sind nun gerade gleich diesen Zahlen.

Corollar 116.1 Voraussetzungen wie im vorigen Satz und $p \geq q+1$.

(i) $p = q+1 \Longrightarrow D_{min} = (q-1)\, p^{n-1}$

(ii) $p > q+1$ und $p \equiv 1 \bmod q+1 \Longrightarrow D_{min} = (q-1)\, \frac{\varphi(2p^n)}{q+1}$

und der Code ist f-äquidistant.

Beweis

(i) Folgt durch Berechnen der Ausdrücke $S2\left(\frac{m}{2p^k}\right)$ und $S2\left(\frac{m}{p^k}\right)$.

(ii) Es gilt $T\left(\frac{m}{2^s p^k}, q+1\right)$ ausgenommen $s = 0$, $k = n$. Dann ist

gp^n einziges Element des Orbits mit dem Gewicht $\varphi(2p^n) = \varphi(p^n)$.

Corollar 116.2 Voraussetzungen wie in Satz 116 aber $q = 3$ und $p > 4$.

$$D_{min} = p^{n-1} \cdot \frac{p-1 - \varepsilon(p)}{2}$$

$$\varepsilon(p) = \begin{cases} 0 & p \equiv 1 \bmod 4 \\ 4 & p \equiv 3 \bmod 4 \end{cases}$$

Beweis Siehe den Beweis zu Corollar 113.2.

Bemerkung

a. Es ist möglich und liegt nahe, Sätze die Satz 111 und Satz 114 entsprechen, abzuleiten.

b. Da gelten muss: $2 \nmid q$, so ist der Fall $m = 2p^n$ in der Literatur bisher nicht untersucht worden.

Satz 117 Sei $m = p_1 \cdot p_2$ $(p_1 < p_2)$, wo p_1, p_2 ungerade Primzahlen sind. Weiter gelte $mg = q^{\lambda} - 1$ mit $\lambda = \langle p_1 - 1, p_2 - 1 \rangle$ und $\omega_q(p_1) = p_1 - 1$, $\omega_q(p_2) = p_2 - 1$ (d. h. q ist primitive Wurzel modulo p_1 und modulo p_2). Dann gilt unter der Voraussetzung $g > q$:

$$D_{min} \leq \operatorname{Min}\left\{ c_2 \cdot SP\left(\frac{m}{p_1}\right),\ c_1 \cdot SP\left(\frac{m}{p_2}\right),\ c_0 \cdot SP\left(\frac{m}{1}\right)\right\} = \triangle$$

$$(i = 1,2) \qquad c_i = \frac{\langle p_1 - 1,\ p_2 - 1\rangle}{p_i - 1}, \qquad c_0 = \frac{1}{(p_1 - 1,\ p_2 - 1)}$$

$$SP\left(\frac{m}{p_1}\right) = \left[q\ \frac{p_2}{q+1}\right] - \left[\frac{p_2}{q+1}\right], \qquad SP\left(\frac{m}{p_2}\right) = \left[q\ \frac{p_1}{q+1}\right] - \left[\frac{p_1}{q+1}\right]$$

$$SP\left(\frac{m}{1}\right) = \left[q\ \frac{p_1 p_2}{q+1}\right] - \left[\frac{p_1 p_2}{q+1}\right] - SP\left(\frac{m}{p_1}\right) - SP\left(\frac{m}{p_2}\right)$$

Beweis Es gilt $\omega_q(p_1 p_2) = \langle \omega_q(p_1), \omega_q(p_2)\rangle = \langle p_1 - 1,\ p_2 - 1\rangle =$

$= \dfrac{(p_1 - 1)\,(p_2 - 1)}{(p_1 - 1,\ p_2 - 1)} = \dfrac{\varphi(p_1 \cdot p_2)}{(p_1 - 1,\ p_2 - 1)}$, wie sich aus bekannten Sätzen der Zahlentheorie ergibt. Die Werte für $SP\left(\frac{m}{p_i}\right)$ $(i = 1,2)$ ergeben sich wie üblich, wenn man beachtet, dass es nur genau zwei Orbits gibt für deren Codepunkte gx man $(x,m) = p_1$ bzw. $(x, m) = p_2$ hat und gp_1 bzw. gp_2 kleinster Repräsentant ist. $SP\left(\frac{m}{1}\right)$ ist gerade die Anzahl der $x \in M_g$ mit $(x, m) = 1$. Sie verteilen sich auf $(p_1 - 1,\ p_2 - 1)$ verschiedene zyklische Klassen $Z(x)$ und es muss gelten $\operatorname{Min}\left\{ \left| Z(x) \cap M_g \right| \;\middle|\; (x, m) = 1 \right\} \leq \dfrac{1}{(p_1 - 1, p_2 - 1)} \cdot SP\left(\frac{m}{1}\right)$.

Satz 118 Voraussetzungen wie im vorigen Satz und zusätzlich noch $(p_1 - 1,\ p_2 - 1) = 2$ sowie $q^{\lambda/2} \not\equiv -1 \bmod m$. Dann gilt:

$$D_{min} = \triangle$$

Beweis Wegen der Voraussetzung $(p_1 - 1,\ p_2 - 1) = 2$ gibt es nur zwei zyklische Klassen $Z(x)$ mit $(x, m) = 1$. Nach Lemma 86 gehört q modulo m nicht zur Klasse C, d.h. wir können die beiden zyklischen Klassen als $Z(1)$ und $Z(-1)$ schreiben. Aus Corollar 106.1

folgt $|Z(1) \cap M_g| = |Z(-1) \cap M_g|$, d.h. jeder Orbit hat genau das Gewicht $\frac{1}{2}$ SP $\left(\frac{m}{1}\right)$.

Lemma 119 Unter denselben Voraussetzungen wie in Satz 117 gilt, wenn $q+1 < p_1 \cdot p_2$

(i) ($p_1 \equiv 1 \bmod q+1$ oder $p_2 \equiv 1 \bmod q+1$)

$$\Longrightarrow c_0 \cdot \mathrm{SP}\left(\frac{m}{1}\right) = (q-1)\ \frac{\langle p_1-1, p_2-1\rangle}{q+1} = (q-1)\ \frac{\varphi(p_1p_2)}{(p_1-1, p_2-1)\ (q+1)}$$

(ii) ($p_1p_2 \equiv -1 \bmod q+1$ und $q+1 \mid \varphi(p_1 \cdot p_2)$) und p_1p_2 ist Nichtausnahmezahl

$$\Longrightarrow c_0 \cdot \mathrm{SP}\left(\frac{m}{1}\right) = (q-1)\ \frac{\langle p_1-1,\ p_2-1\rangle}{q+1} = (q-1)\ \frac{\varphi(p_1p_2)}{(p_1-1, p_2-1)\ (q+1)}$$

(iii) ($p_1 \equiv -1 \bmod q+1$ und $p_2 \equiv -1 \bmod q+1$) $\Longrightarrow$

$$c_0 \cdot \mathrm{SP}\left(\frac{m}{1}\right) = (q-1)\ \frac{\langle p_1-1, p_2-1\rangle - 2}{q+1} = (q-1) \cdot \frac{\varphi(p_1p_2) - 4}{(p_1-1, p_2-1)\ (q+1)}$$

Beweis (i) Die Voraussetzung sagt aus, dass $T(p_1p_2, q+1)$ gilt. Da $\mathrm{SP}\left(\frac{m}{1}\right)$ gerade die Anzahl der Totative von $p_1 \cdot p_2$ im Intervall M_g ist, folgt leicht die Behauptung.

(ii) Ist p_1p_2 Nichtausnahmezahl, so ist die Bedingung $p_1p_2 \equiv -1 \bmod q+1$ und $q+1 \mid \varphi(p_1p_2)$ notwendig und hinreichend für $T(p_1p_2, q+1)$ (siehe Müller [45]). Wir müssen notwendig das gleiche Resultat wie unter (i) erhalten.

(iii) Es gilt (siehe Holzer [30] p. 132 Satz 11)

$$E(q+1, 1, p_1p_2) = \ldots = E(q+1, q-1, p_1p_2) = \mu(p_1p_2)\, \vartheta(p_1p_2) = 4$$

Daraus folgt $c_0 \cdot \mathrm{SP}\left(\frac{m}{1}\right) = (q-1) \cdot (\varphi(p_1p_2) - 4) / q+1$.

Corollar 119.1 Die Voraussetzungen wie in Satz 118 und $q+1 < p_1p_2$, dann gilt:

(i) ($p_1 \equiv 1 \bmod q+1$ und $p_2 \equiv -1 \bmod q+1$) $\Rightarrow D_{min} = (q-1)\ \frac{\langle p_1-1, p_2-1\rangle}{q+1}$

$$= (q-1)\ \frac{\varphi(p_1p_2)}{2\ (q+1)}$$

(ii) $(p_1 \equiv -1 \bmod q+1 \text{ und } p_2 \equiv -1 \bmod q+1) \Longrightarrow$

$$D_{min} = (q-1)\cdot \frac{\langle p_1-1, p_2-1\rangle - 2}{q+1} = (q-1)\cdot \frac{\varphi(p_1p_2) - 4}{2\,(q+1)}$$

Beweis (i) Die Werte für $SP\left(\frac{m}{p_1}\right)$ und $SP\left(\frac{m}{p_2}\right)$ kann man leicht direkt berechnen (siehe Corollar 110.1). Zusammen mit Lemma 119 (i) folgt die Behauptung.

(ii) Wie unter (i), wenn man Lemma 119 (iii) berücksichtigt.

Bemerkung Aus $(p_1-1,\ p_2-1) = 2$ folgt, dass $p_1,\ p_2 \equiv 1 \bmod q+1$ nicht möglich ist.

Corollar 119.2 Voraussetzungen wie in Satz 118, dann gilt:

(i) $(p_1 = q+1 \text{ und } p_2 \equiv 1 \bmod q+1) \Rightarrow D_{min} = (q-1)\ \frac{\langle p_1-1,\ p_2-1\rangle}{q+1}$

(ii) $(p_1 = q+1 \text{ und } p_2 \equiv -1 \bmod q+1) \Rightarrow D_{min} = (q-1)\ \frac{\langle p_1-1,\ p_2-1\rangle - 1}{q+1}$

Beweis Folgt durch direkte Berechnung von $SP\left(\frac{m}{p_i}\right)$ $(i = 1,2)$ und $SP\left(\frac{m}{1}\right)$.

Bemerkung

a. In den beiden Fällen $q = 2,\ 3,\ 5$ ist nur $p_i \equiv \pm 1 \bmod q+1$ möglich (ausgenommen $p_1 = q+1$). Dann haben wir sämtliche Werte für D_{min} bestimmt. Will man ganz allgemein geschlossene Ausdrücke für D_{min} bestimmen, so ist es nötig $E\ (q+1\ ,\ j,\ p_i)$ $(i = 1,2)$ und $E\ (q+1,\ j,\ p_1p_2)$ für $j = 1,\ \ldots,\ q-1$ zu kennen (wobei $q+1 < p_1$ gelten soll). Schon für $q = 4$ ist eine Berechnung dieser Größen sehr schwierig.

b. Für $q = 2$ finden sich unsere Ergebnisse schon bei Tsao-Wu [66].

c. Nur unwesentlich ändern sich alle Überlegungen, wenn man die Voraussetzungen in Satz 118 wie folgt modifiziert: q sei primitive Wurzel modulo p_1, $-q$ primitive Wurzel modulo p_2, $\left(p_1-1,\ \frac{p_2-1}{2}\right) = 1$ und $q^{\lambda/2} \not\equiv -1 \bmod m$, mit $\lambda = \langle p_1-1,\ \frac{p_2-1}{2}\rangle =$ $= \frac{(p_1-1)\,(p_2-1)}{2}$. Es dürfte klar sein, dass sich für D_{min} die

gleichen Werte ergeben.

Satz 120 Sei $m = p_1^{\alpha_1} p_2^{\alpha_2}$ $(\alpha_1, \alpha_2 > 1,\ p_1 < p_2)$, wo p_1, p_2 ungerade Primzahlen sind. Weiter sei $mg = q^{\lambda}-1$ mit $\lambda = \langle \varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}) \rangle$ und $\omega_q(p_1^{\alpha_1}) = \varphi(p_1^{\alpha_1})$, $\omega_q(p_2^{\alpha_2}) = \varphi(p_2^{\alpha_2})$ (q ist primitive Wurzel modulo $p_1^{\alpha_1}$ und $p_2^{\alpha_2}$) und $(p_1-1,\ p_2-1) = 2$, sowie $q^{\lambda/2} \not\equiv -1 \bmod m$. Dann gilt unter der Voraussetzung $g > q$:

$$D_{min} = \mathrm{Min} \left\{ c_2 \cdot SP1\left(\frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k}}\right),\ c_1 \cdot SP2\left(\frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2}}\right),\right.$$

$$\left. c_{1,2} \cdot SP3\left(\frac{m}{p_1^{\alpha_1-k_1} p_2^{\alpha_2-k_2}}\right) \right| \begin{array}{l} k = 1, \ldots, \alpha_2; \\ s = 1, \ldots, \alpha_1;\ k_1 = 1, \ldots, \alpha_1; \\ k_2 = 1, \ldots, \alpha_2 \end{array} \Big\}$$

$$c_2 = \frac{\varphi(p_1^{\alpha_1})}{2} \cdot p_2^{\alpha_2-k}, \quad c_1 = \frac{\varphi(p_2^{\alpha_2})}{2} \cdot p_1^{\alpha_1-s}, \quad c_{1,2} = \frac{1}{2} p_1^{\alpha_1-k_1} p_2^{\alpha_2-k_2}$$

$$SP1\left(\frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k}}\right) = \left[q \cdot \frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k} (q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k} (q+1)}\right]$$

$$- \left\{\left[q \cdot \frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k} \cdot p_2 (q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1} p_2^{\alpha_2-k} \cdot p_2\ (q+1)}\right]\right\}$$

$$SP2\left(\frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2}}\right) = \left[q \cdot \frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2} (q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2} \cdot (q+1)}\right]$$

$$- \left\{\left[q \cdot \frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2} \cdot p_1\ (q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-s} p_2^{\alpha_2} \cdot p_1\ (q+1)}\right]\right\}$$

$$SP^3\left(\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}}\right) = \left[q\cdot\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}(q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}(q+1)}\right]$$

$$-\left\{\left[q\cdot\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_1(q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_1(q+1)}\right]\right\}$$

$$-\left\{\left[q\cdot\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_2(q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_2(q+1)}\right]\right\}$$

$$+\left\{\left[q\cdot\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_1p_2(q+1)}\right] - \left[\frac{m}{p_1^{\alpha_1-k_1}p_2^{\alpha_2-k_2}\cdot p_1p_2(q+1)}\right]\right\}$$

Beweis Ist gx ein Codepunkt und (x, m) = d, so kommen für d nur die Werte $p_1^{\alpha_1}\cdot p_2^{\alpha_2-k}$, $p_1^{\alpha_1-s}\cdot p_2^{\alpha_2}$ und $p_1^{\alpha_1-k_1}\cdot p_2^{\alpha_2-k_2}$ in Frage. Wir müssen wie üblich, alle $x' \in M_g/d$ mit (x', m/d) = 1 bestimmen. Dies sind gerade die Zahlen SP1, SP2, SP3, wie man sich leicht überlegt.

Ist $d = p_1^{\alpha_1}p_2^{\alpha_2-k}$, $p_1^{\alpha_1-s}p_2^{\alpha_2}$, so ist gd kleinster Repräsentant des einzigen Orbits, denn q ist primitive Wurzel modulo p_1^s, p_2^k und $|Z(p_1^{\alpha_1}p_2^{\alpha_2-k})\cap M_g| = SP1\left(\frac{m}{p_1^{\alpha_1}p_2^{\alpha_2-k}}\right)$ und entsprechend für $d = p_1^{\alpha_1-s}p_2^{\alpha_2}$. Die Faktoren c_1, c_2 sind gerade gleich $\lambda/\omega_q(m/d)$:

$$c_2 = \frac{\langle\varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2})\rangle}{\omega_q(p_2^k)} = \frac{\varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})}{\varphi(p_2^k)\ \ (\varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2}))}$$

$$= \frac{\varphi(p_1^{\alpha_1})}{2}\cdot p_2^{\alpha_2-k}$$

denn aus $(p_1-1,\ p_2-1) = 2$ folgt $(\varphi(p_1^{\alpha_1}),\ \varphi(p_2^{\alpha_2})) = 2$; und ganz entsprechend berechnet man c_1.

Ist $d = p_1^{\alpha_1-k_1} \cdot p_2^{\alpha_2-k_2}$ so gibt es genau zwei Orbits, denn

$$\frac{\varphi(m/d)}{\omega_q(m/d)} = \frac{\varphi(p_1^{k_1} p_2^{k_2})}{\langle \varphi(p_1^{k_1}), \varphi(p_2^{k_2}) \rangle} = 2$$

Nach Lemma 86 gehört q modulo $m/d = p_1^{k_1} p_2^{k_2}$ nicht zur Klasse C, aus $q^{\lambda_d/2} \equiv -1 \bmod m/d$, mit $\lambda_d = \omega_q(m/d) = \frac{\varphi(p_1^{k_1} p_2^{k_2})}{2}$ würde folgen $q^{\lambda/2} \equiv -1 \bmod m$ im Widerspruch zur Voraussetzung. Wir wollen die letzte Behauptung noch beweisen:

$$q^{\lambda_d/2} \equiv -1 \bmod p_1^{k_1} p_2^{k_2} \Longrightarrow q^{\lambda_d/2} \equiv -1 \bmod p_1^{k_1}, p_2^{k_2}$$

$$\Longrightarrow q^{\lambda_d/2 \cdot p_1^{\alpha_1-k_1}} \equiv (-1)^{p_1^{\alpha_1-k_1}} \bmod p_1^{k_1+(\alpha_1-k_1)} \text{ (vgl. Le Veque [36] Theorem 4-5, p. 50)}$$

und $q^{\lambda_d/2 \cdot p_2^{\alpha_2-k_2}} \equiv -1 \bmod p_2^{\alpha_2}$ $\left(\lambda_d \cdot p_1^{\alpha_1-k_1} = \frac{\varphi(p_1^{\alpha_1} p_2^{k_2})}{p_2^{\alpha_2-k_2}}\right.$ und entsprechend $\left.\lambda_d \cdot p_2^{\alpha_2-k_2}\right)$

$$\Longrightarrow q^{\lambda_d/2 \cdot p_1^{\alpha_1-k_1} \cdot p_2^{\alpha_2-k_2}} \equiv -1 \bmod p_1^{\alpha_1} \text{ und } q^{\lambda_d/2 \cdot p_2^{\alpha_2-k_2} \cdot p_1^{\alpha_1-k_1}} \equiv -1 \bmod p_2^{\alpha_2}$$

$$\left(\lambda_d \cdot p_1^{\alpha_1-k_1} \cdot p_2^{\alpha_2-k_2} = \frac{\varphi(p_1^{\alpha_1} p_2^{\alpha_2})}{2} !\right)$$

$$\Longrightarrow q^{\lambda/2} \equiv -1 \bmod p_1^{\alpha_1} p_2^{\alpha_2} \quad \text{Widerspruch!}$$

Damit sind 1 und -1 Repräsenanten der zwei zyklischen Klassen modulo m/d. Jeder Orbit hat dann wieder das Gewicht 1/2 $\varphi(m/d)$. Weiter gilt

$$\frac{\lambda}{\omega_q(m/d)} = p_1^{\alpha_1-k_1} \cdot p_2^{\alpha_2-k_2}$$

zusammen mit dem Faktor 1/2 ergibt sich der Wert für $c_{r,s}$.

Corollar 120.1 Voraussetzungen wie im vorigen Satz und $p_1 > q+1$ Dann gilt:

(i) $(p_1 \equiv 1 \bmod q+1$ und $p_2 \equiv -1 \bmod q+1) \Longrightarrow$

$$D_{min} = (q-1)\ \frac{\varphi(p_1^{\alpha_1 \alpha_2}) - 2\,\varphi(p_1^{\alpha_1})\ p_2^{\alpha_2-2}}{2\ (q+1)}$$

(ii) In den Fällen $p_1 \equiv -1$, $p_2 \equiv 1 \bmod q+1$ sowie p_1, $p_2 \equiv -1 \bmod q+1$ folgt,

$$D_{min} = (q-1)\ \frac{\varphi(p_1^{\alpha_1 \alpha_2}) - 2\,\varphi(p_2^{\alpha_2})\ p_1^{\alpha_1-2}}{2\ (q+1)}$$

wobei man beachte, dass p_1, $p_2 \equiv 1 \bmod q+1$ wegen $(p_1-1,\ p_2-1) = 2$ nicht möglich ist.

Beweis Folgt mit Hilfe der Theorie der Totative bzw. durch direkte Berechnung, unter Beachtung von: $p_1 < p_2$ und p_1 ist ungerade Primzahl.

Corollar 120.2 Voraussetzungen wie in Satz 120 und $p_1 = q+1$, $p_2 \equiv 1 \bmod q+1$. Dann gilt,

$$D_{min} = (q-1)\ \frac{\varphi(p_1^{\alpha_1}\ p_2^{\alpha_2})}{2\ (q+1)}$$

für alle Codepunkte bis auf die Punkte $g\ p_1^{\alpha_1-1}\ p_2^{\alpha_2} \cdot x'$ $(x'=1, \ldots, p_1-1)$

Sie besitzen das modulare Gewicht $(q-1)\ \frac{\varphi(p_2^{\alpha 2})}{2\ (q+1)} \cdot p_1^{\alpha_1} = W(p_1)$

und es ist $D_{min}/W(p_1) = 1 - \frac{1}{p_1}$.

Beweis Man erkennt leicht, dass sämtliche Orbits das Gewicht D_{min} haben, bis auf den Orbit mit $d = p_1^{\alpha_1-1}\ p_2^{\alpha_2}$, dessen Gewicht $(q-1) \cdot c_1 = W(p_1)$ ist.

Bemerkung

a. In den Fällen q = 2, 3, 5 ist nur $p_i \equiv \pm 1 \bmod q+1$ möglich (ausgenommen $p_1 = q+1$). Will man allgemein geschlossene Ausdrücke für D_{min} bestimmen, so müssen wir wieder $E(q+1, j, p_1^s)$ bzw. $E(q+1, j, p_2^k)$ und $E(q+1, j, p_1^{k_1} p_2^{k_2})$ kennen.

b. In Corollar 120.2 haben wir eine Klasse von Codes vor uns, die wir a(symptotisch)-äquidistant nennen wollen. Denn mit wachsendem p_1, also auch q, strebt $D_{min}/W(p_1)$ gegen 1.

c. Für q = 2 sind die in Corollar 120.1 angegebenen Werte von D_{min} ebenfalls schon von Tsao-Wu [66] angegeben worden.

d. Für q = 2 haben unabhängig von den angegebenen amerikanischen Autoren auch russische Autoren versucht D_{min} zu bestimmen. (siehe Dadaev [17] und Tenengolts/Dynkin [65]). Da sie direkte Methoden benutzen, sind die Ergebnisse etwas schwächer.

Satz 121 Sei $g \cdot m = q^\lambda - 1$, $\lambda = \omega_q(m)$ und $m = \prod_{i=1}^{h} p_i^{\alpha_i}$ (p_i Primzahl). Ist $m > q+1$, so gilt für W(m), die Summe über alle $|Z(x) \cap M_g|$ mit (x, m) = 1 wo die gx Repräsentanten aller $\varphi(m)/\omega_q(m)$ verschiedenen Orbits sind,

$$W(m) = (q-1)\,\frac{\varphi(m)}{q+1}$$

unter den folgenden Bedingungen:

(i) $(q+1)^2 \mid m$

(ii) $p_i \equiv 1 \bmod q+1$ für ein $1 \leq i \leq h$.

(iii) $m \equiv 0 \bmod q+1$ und m und $\frac{m}{q+1}$ haben dieselben Primfaktoren.

(iv) $2m \equiv 0 \bmod q+1$ und m und $\frac{2m}{q+1}$ haben dieselben Primteiler.

(v) $q+1 = 2p$ (p ungerade Primzahl) und $\varphi(m) \equiv 0 \bmod q+1$.

(vi) $q+1 = p^\alpha$ (p ungerade Primzahl, $\alpha > 1$) und $m = m_1 p^{\alpha+1}$, $(m_1, p) = 1$.

Beweis Die Summe über $|Z(x) \cap M_g|$ für alle $\varphi(m)/\omega_q(m)$ verschiedene Orbits ist gleich der Anzahl aller $n \in M_g = \left(\frac{m}{q+1}, q \cdot \frac{m}{q+1}\right]$ mit (n, m) = 1. Aus der Theorie der Totative ist bekannt, dass aus

den Bedingungen (i) - (vi) die Gleichverteilung der Totative von m folgt (siehe Holzer [30]). Aus dieser Bemerkung ergibt sich sofort die Behauptung.

Satz 122 Die Voraussetzungen wie im vorigen Satz und q = 2. Dann gilt:

(i) $p_i \equiv -1 \bmod 3$ für alle $i = 1, \ldots, h \Longrightarrow$

$$W(m) = \frac{\varphi(m) - (-1)^{\sum \alpha_i} \cdot 2^h}{3}$$

(ii) $3 \nmid m \Longrightarrow W(m) = \frac{\varphi(m) - (-1)^{\sum \alpha_i} 2^{h-1}}{3}$

Beweis Die Bedingungen in (i) bzw. (ii) bedeuten gerade, dass m Nichtausnahmezahl bezüglich q+1 ist. Dann kann man wie im Beweis zu Corollar 113.1 E(3, 1, m) berechnen und daraus die Anzahl der Totative von m in M_g bestimmen.

Satz 123 Die Voraussetzungen wie in Satz 121 und q = 3. Dann gilt:

(i) $4 \mid m$ oder $p_1 \equiv 1 \bmod 4$ für ein $1 \leq i \leq h \Longrightarrow W(m) = 3 \cdot \frac{\varphi(m)}{4}$

(ii) Ist keine der Bedingungen unter (i) erfüllt, so

$$W(m) = \begin{cases} \frac{\varphi(m) - (-1)^{\sum \alpha_i} 2^{h+1}}{4} & \text{falls } m \equiv 1 \bmod 2 \\ \frac{\varphi(m) - (-1)^{\sum \alpha_i} 2^h}{4} & \text{falls } m \equiv 2 \bmod 4 \end{cases}$$

Beweis Berechnung von E (4,1,m) = E (4,2,m) = -E (4,0,m) ganz analog wie im vorigen Satz.

Corollar 122.1 Voraussetzungen wie in Satz 121 und $q < g$. Ist dann eine der Bedingungen (i) - (vi) erfüllt, so gilt:

$$D_{min} \leq (q-1) \frac{\omega_q(m)}{q+1}$$

und diese Abschätzung ist scharf.

Beweis Es gibt genau $\varphi(m) / \omega_q(m)$ Orbits mit (x, m) = 1 = d

und daraus folgt $D_{min} \leq W(m) \Big/ \frac{\varphi(m)}{\omega_q(m)}$. Wegen Satz 121 gilt dann die Behauptung. Diese Abschätzung ist scharf, denn nach Corollar 110.1 wird die Schranke für $m = p$, $p \equiv 1 \bmod q+1$ und $\omega_q(p) = p-1$ angenommen.

Lemma 124 Sei $g \cdot m = q^{\lambda} - 1$, $\lambda = \omega_q(m)$ und $g > q$. Dann gilt

$$D_{min} \leq W(m) \cdot \frac{\omega_q(m)}{\varphi(m)}$$

und die Abschätzung ist scharf.

Beweis Siehe den Beweis des letzten Corollars.

Bemerkung

a. Für $q = 2$ haben Chien/Hong/Preparata [12], auf prinzipiell anderem Wege, die entsprechenden Werte aus Satz 122 und Satz 123 gefunden. Die Abschätzung in Corollar 122.1 hat zuerst Tsao-Wu [66] für $q = 2$ und $m = p$ angegeben.

b. Will man für $q > 3$ zu vollständigen Fallunterscheidungen kommen, so muss man wieder $E(q+1, j, m)$ für $j = 1, \ldots, q-1$ berechnen.

c. Es dürfte klar sein, dass man für $(x, m) = d$ entsprechende Ergebnisse wie in Satz 121 erhält.

4.5 Zyklische Codes hoher Rate

Definition 34 Seien $p_1, p_2, \ldots, p_n$ ungerade Primzahlen mit $(p_i, q) = 1$, $2 \leq q$ und

$$\langle \omega_q(p_1), \ldots, \omega_q(p_n) \rangle = c \cdot \prod_{i=1}^{n} p_i^{\delta_i} \quad , \quad (c, p_i) = 1 \text{ für alle } i.$$

Dann heisst

$$S = S(p_1, \ldots, p_n) = \prod_{i=1}^{n} p_i^{\delta_i + 1} \qquad (\delta_i \geq 0)$$

das Saturations-Produkt der p_i ($i = 1, \ldots, n$) (kurz: S-Produkt).

Definition 35 Eine ungerade Primzahl, mit $(p, q) = 1$, $2 \leq q$ wird q-regulär genannt, wenn $p \parallel q^{p-1} - 1$ gilt.

Bemerkungen a. Für $2 \leq q \leq 10$ und $p < 500\,000$ sind nach Riesel [59] nur die unten tabellierten Primzahlen nicht q-regulär.

q	p	q	p
2	1093, 3511	6	66 161
3	11	7	5, 491531
4	1093, 3511	8	3, 1093, 3511
5	20771, 40487	9	11
		10	3, 487

b. Von nun an bis zum Ende dieses Abschnitts sollen alle betrachteten Primzahlen q-regulär sein.

Satz 125 Sei $m = \prod_{i=1}^{n} p_i^{\alpha_i}$ ($\alpha_i \geq 1$ für alle i), $(q, m) = 1$, $2 \leq q$.

Dann ist $\omega_q(m) = \omega_q(S)$

wenn gilt $m \mid S(p_1, \ldots, p_n)$.

Beweis $\omega_q(S) = \langle \omega_q(p_1^{\beta_1+1}), \ldots, \omega_q(p_n^{\beta_n+1}) \rangle$

$\omega_q(p_i^{\beta_i+1}) = \omega_q(p_i) \cdot p_i^{\max(0, \beta_i+1-z)} \cdot p_i^{z} \Big\|_q^{\lambda_i - 1}$

mit $\lambda_i = \omega_q(p_i)$ und $\lambda_i \mid p_i - 1$. Da alle p_i q-regulär sind muss $z = 1$ gelten:

$$\omega_q(p_i^{\beta_i+1}) = \omega_q(p_i) \cdot p_i^{\beta_i}$$

$$\omega_q(S) = \langle \omega_q(p_1) \cdot p_1^{\beta_1}, \ldots, \omega_q(p_n) \cdot p_n^{\beta_n} \rangle$$

$$= \langle \prod p_i^{\beta_i}, \langle \omega_q(p_1), \ldots, \omega_q(p_n) \rangle \rangle$$

$$= c \cdot \prod p_i^{\beta_i}$$

$$\omega_q(m) = \langle \omega_q(p_1^{\alpha_1}), \ldots, \omega_q(p_n^{\alpha_n}) \rangle$$

$$= \langle \prod p_i^{\alpha_i - 1}, \langle \omega_q(p_1), \ldots, \omega_q(p_n) \rangle \rangle$$

$$= c \cdot \prod p_i^{\beta_i} \qquad \text{wegen } 1 \leq \alpha_i \leq \beta_i + 1$$

$$= \omega_q(S)$$

Satz 126 Ist $m = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$, $(m, q) = 1$ und $S(p_1,\ldots,p_n) \mid m$, so gilt:

(i) $\omega_q(m) \cdot S = \omega_q(S) \cdot m$

(ii) $\frac{\varphi(m)}{\omega_q(m)} = \frac{\varphi(S)}{\omega_q(S)}$

Beweis (i) Aus dem Beweis des vorigen Satzes entnimmt man leicht

$$\omega_q(m) = c \cdot \prod p_i^{\max(\alpha_i-1,\delta_i)} = c \cdot \prod p_i^{\alpha_i-1}$$

woraus schon die Behauptung folgt.

(ii) $$\frac{\varphi(m)}{\omega_q(m)} = \frac{\prod p_i^{\alpha_i-1}(p_i-1)}{c \cdot \prod p_i^{\alpha_i-1}} = \frac{\prod(p_i-1)}{c} = \frac{\varphi(S)}{\omega_q(S)}$$

Satz 127 Seien $p_1, \ldots, p_n$ ungerade Primzahlen und $m = \prod_{i=1}^{n} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$, $mg = q^{\lambda} - 1$ mit $\lambda = \omega_q(m)$. In der Klasse aller AN-Codes besitzt der Code mit $m = S(p_1, \ldots, p_n)$ maximale Rate $Rt(m)$.

Beweis

$$Rt(m) = \frac{\log_q m}{\log_q(q^{\lambda}-1)} \sim \frac{\log_q m}{\omega_q(m)} = \frac{\sum \alpha_i \log_q p_i}{c \cdot \prod p_i^{\max(\alpha_i-1,\ \delta_i)}}$$

Wir unterscheiden die Fälle $m \mid S$, dann ist wegen Satz 125 die Behauptung klar, und $S \mid m$. Nach Satz 126 (i) wächst dann der Nenner stärker als der Zähler, was wiederum die Behauptung zeigt.

Bemerkung

Das S-Produkt wurde von Chien [11] eingeführt. Die Sätze sind Verallgemeinerungen auf $q \geq 2$ von entsprechenden Aussagen bei Chien/Hong/Preparata [12].

Lemma 128 Die Voraussetzungen wie in Satz 125 und $m' = \prod_{i=1}^{n} p_i^{\beta_i}$ ($\beta_i \geq 0$), $m' \mid S$. Dann gilt

$$m' \neq m \text{ und } m' \mid m \Longrightarrow D_{min}\left[\|\|_{q(mg)}\ (\overline{g})\right] = D_{min}\left[\|\|_{q(m'g')}\ (\overline{g'})\right]$$

$$\text{und } Rt(m) > Rt(m')$$

wobei $mg = m'g' = q^{\lambda} - 1$ mit $\lambda = \omega_q(m) = \omega_q(m') = \omega_q(S)$ und $g, g' > q$ ist.

Beweis Der erste Teil der Behauptung folgt aus Lemma 107, der zweite Teil direkt aus der Definition von Rt.

Bemerkung

Lemma 128 ist von gewisser praktischer Bedeutung, denn aus ihm folgt, dass unter Umständen die Coderate erhöht werden kann ohne D_{min} zu senken. Dies kann durch eine systematische Suche geschehen, die auf einem Rechner programmiert werden kann (vgl. Chien/Hong/Preparata [12]).

Definition 36 Ein AN-Code mit $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$ und $S(p_1, \ldots, p_n) \mid m$ heisst augmentierter Code.

Definition 37 Sei $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$, dann heisst m saturiert bezüglich $p_1, \ldots, p_n$, wenn $\alpha_i \geq \delta_i + 1$ für $i = 1, \ldots, n$ gilt und $1 \leq \alpha_i \leq \delta_i$ für $i = n+1, \ldots, n+k$ gilt. Dabei ist

$$S(p_1, \ldots, p_{n+k}) = \prod_{i=1}^{n+k} p_i^{\delta_i + 1}$$ das S-Produkt der $p_1, \ldots, p_{n+k}$.

Lemma 129 Sei $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$ saturiert bezüglich $p_1, \ldots, p_n$, dann gilt:

(i) $$\omega_q\left(m \cdot \prod_{i=1}^{n} p_i^{\beta_i}\right) = \omega_q(m) \cdot \prod_{i=1}^{n} p_i^{\beta_i} \qquad (\beta_i \geq 0)$$

(ii) $$\frac{\varphi(m)}{\omega_q(m)} = \frac{\varphi\left(m \cdot \prod_{i=1}^{n} p_i^{\beta_i}\right)}{\omega_q\left(m \cdot \prod_{i=1}^{n} p_i^{\beta_i}\right)}$$

Beweis Ähnlich wie die Beweise in Satz 125 und Satz 126.

Lemma 130 Sei $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$ saturiert bezüglich $p_1, \ldots, p_n$, dann existiert eine bijektive Abbildung der Orbits von m mit d = 1 auf die Orbits von $m' = m \cdot \prod_{i=1}^{n} p_i^{\beta_i}$ mit d = 1. Ist Z(x) eine zyklische Klasse bezüglich m mit (x, m) = 1, so ist

$$Z(x) = \left\{ p_i(x) + \gamma \cdot m \;\middle|\; 0 \leq i < \omega_q(m),\ 0 \leq \gamma < \prod_{i=1}^{n} p_i^{\beta_i} \right\}$$

die zugeordnete zyklische Klasse bezüglich m'.

Beweis Es genügt, wenn wir die letzte Behauptung zeigen.

Aus (x, m) = 1 folgt (x, m') = 1, und aus $q^{\omega_q(m)\cdot i} \equiv 1 \bmod m$ ergibt sich $q^{\omega_q(m)\cdot i} - 1 = \gamma_i \cdot m$ ($\gamma_i \geq 0$). Weiter folgt

$$x(q^{\omega_q(m)\cdot i} - 1) = x \cdot \gamma_i \cdot m \equiv \gamma_i' \cdot m \bmod m' \text{ mit } 0 \leq \gamma_i' < \prod_{i=1}^{n} p_i^{\beta_i}.$$

Da $\omega_q(m') = \omega_q(m) \cdot \prod_{i=1}^{n} p_i^{\beta_i}$ (siehe Lemma 129 (i)), so gilt:

$\gamma_i' = \gamma_j' \Longleftrightarrow i \equiv j \bmod \prod_{i=1}^{n} p_i^{\beta_i}$. Insgesamt hat man die Behauptung, wenn man beachtet, dass nach Lemma 129 (ii) die Anzahl der Orbits bezüglich m und m' gleich ist.

Satz 131 Sei $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$ saturiert bezüglich $p_1, \ldots, p_n$ und $m' = m \cdot \prod_{i=1}^{n} p_i^{\beta_i}$. Weiter sei $g \cdot m = q^{\lambda} - 1$, $\lambda = \omega_q(m)$ und $g' \cdot m' = q^{\lambda'} - 1$, $\lambda' = \omega_q(m') = \lambda \cdot \prod_{i=1}^{n} p_i^{\beta_i}$. Ist (x, m') = 1, so gilt:

(i) $|Z(x) \cap M_{g'}| = (q-1)\ \dfrac{\omega_q(m')}{q+1}$ wenn $\prod_{i=1}^{n} p_i^{\beta_i} \equiv 0 \bmod q+1$

(ii) $|Z(x) \cap M_{g'}| = (q-1) \cdot \dfrac{\omega_q(m') - \omega_q(m)}{q+1} + |Z(x) \cap M_g|$

falls $\prod_{i=1}^{n} p_i^{\beta_i} \equiv 1 \bmod q+1$

(iii) $|Z(x) \cap M_{g'}| = (q-1) \cdot \frac{\omega_q(m') + \omega_q(m)}{q+1} - |Z(x) \cap M_g|$

wenn $\prod_{i=1}^{n} p_i^{\beta_i} \equiv -1 \bmod q+1$

Beweis Die Behauptung folgt aus Lemma 130 mittels elementarer aber etwas verwickelter Überlegungen. So ergibt sich z.B. (i) aus $|Z(x)| = \omega_q(m)$, $M_{g'} = \left(m \cdot \frac{\prod \beta_i}{q+1}, m \cdot q \cdot \frac{\prod \beta_i}{q+1}\right]$, d.h. $M_{g'}$ hat die Länge $L = \left((q-1) \cdot \frac{\prod \beta_i}{q+1}\right) \cdot m$ und nach Lemma 130 können wir jedes Element aus $Z(x)$ genau L mal nach $M_{g'}$ "verschieben", woraus mit Lemma 129 (i) die Behauptung folgt.

Lemma 132 Voraussetzungen wie in Lemma 130. Sei $d' | m'$, wo

$$d' = \prod_{i=1}^{n'} p_i^{\beta_i'} \prod_{i=n'+1}^{n} p_i^{\beta_i} \prod_{i=n'+1}^{n+k} p_i^{\gamma_i} \quad \text{mit } 1 \leq n' \leq n,\ 0 \leq \beta_i' < \beta_i,$$

$0 \leq \gamma_i \leq \alpha_i$.

Ist $d = \prod_{i=n'+1}^{n+k} p_i^{\gamma_i}$ und $(x', m) = d$, $x = x'/d$, $\delta_i = \beta_i - \beta_i'$ so gilt für $Z(xd')$ die zyklische Klasse bezüglich m',

$$Z(xd') = d' \cdot \left\{ R_{m/d}(xq^i) + \gamma \cdot m/d \mid 0 \leq i < \omega_q(m/d),\ 0 \leq \gamma < \prod_{i=1}^{n'} p_i^{\delta_i} \right\}$$

Für gegebenes d' ist die Zuordnung zwischen den Orbits von m' und den Orbits von m mit $(x, m) = d$ umkehrbar eindeutig.

Beweis Der Beweis verläuft ganz ähnlich wie in Lemma 130. Es braucht nur noch beachtet zu werden,

$$m/d = \prod_{i=1}^{n'} p_i^{\alpha_i} \cdot \prod_{i=n'+1}^{n+k} p_i^{\gamma_i'}, \quad \gamma_i' = \alpha_i - \gamma_i$$

$$m'/d' = m/d \cdot \prod_{i=1}^{n'} p_i^{\delta_i}$$

und m/d ist saturiert bezüglich $p_1, \ldots, p_{n''}$, $n' \leq n'' \leq n$, so dass man Lemma 130 anwenden kann.

Satz 133 Die Voraussetzungen wie in Satz 131, sowie d und d' wie im vorigen Lemma, mit den entsprechenden Bezeichnungen.

(i) $|Z(xd') \cap M_{g'}| = (q-1)\ \frac{\omega_q(m'/d')}{q+1}$ wenn $\prod_{i=1}^{n'} p_i^{\delta_i} \equiv 0 \bmod q+1$

(ii) $|Z(xd') \cap M_{g'}| = (q-1)\ \frac{\omega_q(m'/d') - \omega_q(m/d)}{q+1} + |Z(xd) \cap M_g|$

falls $\prod_{i=1}^{n'} p_i^{\delta_i} \equiv 1 \bmod q+1$

(iii) $|Z(xd') \cap M_{g'}| = (q-1)\ \frac{\omega_q(m'/d') + \omega_q(m/d)}{q+1} - |Z(xd) \cap M_g|$

wenn $\prod_{i=1}^{n'} p_i^{\delta_i} \equiv -1 \bmod q+1$

Beweis Dieser Satz ist eine Verallgemeinerung von Satz 131 und folgt leicht aus Lemma 132.

Lemma 134 m und m' seien wie in Satz 131 definiert. Ein Teiler d' von m' kann genau von einer der folgenden beiden Formen sein:

$$d' = \begin{cases} \prod_{i=1}^{n} p_i^{\beta_i} \cdot d,\ d \mid m & \text{Teiler 1. Art} \\ \prod_{i=1}^{n'} p_i^{\beta_i'} \cdot \prod_{i=n'+1}^{n} p_i^{\beta_i} \cdot \prod_{i=n'+1}^{n+k} p_i^{\gamma_i},\ 1 \le n' \le n, & \\ \qquad 0 \le \beta_i' < \beta_i,\ 0 \le \gamma_i < \alpha_i & \text{Teiler 2. Art} \end{cases}$$

Ist d' von der Form $d' = \prod_{i=1}^{n} p_i^{\beta_i} \cdot d$ (1. Art), so gilt, wenn $(x', m') = d'$ und $x = x'/d'$ ist:

$$|Z(xd') \cap M_{g'}| \cdot \frac{\omega_q(m')}{\omega_q(m'/d')} = |Z(xd) \cap M_g| \cdot \frac{\omega_q(m)}{\omega_q(m/d)} \cdot \prod_{i=1}^{n} p_i^{\beta_i}$$

Beweis Dass die Teiler von m' nur die beiden angegebenen Formen haben können, überlegt man sich leicht. Aus $m/d = m'/d'$ folgt

$$|Z(xd') \cap M_{g'}| = |Z(xd) \cap M_g|$$

und der Rest aus Lemma 129 (i).

Satz 135 Sei $m = \prod_{i=1}^{n+k} p_i^{\alpha_i}$ saturiert bezüglich $p_1, \ldots, p_n$ und $m' = \prod_{i=1}^{n} p_i^{\beta_i} \cdot m$. Es gelte $p_i \equiv 1 \bmod q+1$ für alle $1 \leq i \leq n$ oder $p_i = q+1$ für alle $1 \leq i \leq n$, vorausgesetzt $(q+1)^2 | m$. Dann gilt, wenn $g, g' > q$ ist

$$D_{min}\left[\| \|_{q(m'g')}\ (\overline{g'})\right] = \prod_{i=1}^{n} p_i^{\beta_i} \cdot D_{min}\ \left[\| \|_{q(mg)}\ (\overline{g})\right]$$

Beweis Ist d' ein Teiler 1. Art von m' der Form $d' = \prod_{i=1}^{n} p_i^{\beta_i} \cdot d$ $(d|m)$, so können wir uns auf das Ergebnis von Lemma 134 stützen und wegen Satz 106 genügt es zu zeigen

$$(6)\quad \min_{\substack{x \\ (x,\ m/d')=1}} \left\{ |Z(xd') \cap M_{g'}| \cdot \frac{\omega_q(m')}{\omega_q(m'/d')} \right\} \geq \min_{\substack{x \\ (x,\ m/d)=1}} \left\{ |Z(xd) \cap M_g| \cdot \frac{\omega_q(m')}{\omega_q(m/d)} \right\}$$

wo d' ein Teiler 2. Art von m' ist. Wir setzen die Ungleichung (6) vorerst als Richtig voraus und beweisen die Behauptung. Zunächst gilt

$$D_{min}\left[\| \|_{q(m'g')}(\overline{g'})\right] \leq \prod_{i=1}^{n} p_i^{\beta_i}\ D_{min}\left[\| \|_{q(mg)}\ (\overline{g})\right]$$

denn ist d derjenige Teiler von m für den D_{min} angenommen wird und $(x, m/d) = 1$ der entsprechende x-Wert, so ist $d' = d \cdot \prod_{i=1}^{n} p_i^{\beta_i}$ ein Teiler von m'. Aus Lemma 134 folgt dann schon alles.

Sei nun umgekehrt d' der Teiler von m' für den D_{min} angenommen wird. Ist d' ein Teiler 1. Art, so folgt aus Lemma 134

$$(7)\quad D_{min}\left[\| \|_{q(m'g')}(\overline{g'})\right] \geq \prod_{i=1}^{n} p_i^{\beta_i}\ D_{min}\left[\| \|_{q(mg)}\ (\overline{g})\right]$$

und alles ist gezeigt. Ist d' ein Teiler 2. Art von m', so zeigt die Ungleichung (6), dass ebenfalls (7) gilt.

Wir beweisen nun die Ungleichung (6). Wegen der Voraussetzungen können wir Satz 121 zur Bestimmung von W (m/d) bzw. W (m'/d') heranziehen. Dies ergibt

$$\min_x \left\{ |Z(xd) \cap M_g| \right\} \leq \frac{W(m/d)}{\frac{s(m/d)}{\omega_q(m/d)}} = (q-1) \frac{\omega_q(m/d)}{q+1}$$

m/d ist saturiert bezüglich $p_1, \ldots, p_{n''}$ mit $n' \leq n'' \leq n$, also nach Satz 133 entweder

$$\min_x \left\{ |Z(xd') \cap M_{g'}| \right\} = (q-1) \frac{\omega_q(m'/d')}{q+1} = (q-1) \frac{\omega_q(m/d)}{q+1} \cdot \prod_{i=1}^{n'} p_i^{\delta_i}$$

$$\geq \min_x \left\{ |Z(xd) \cap M_g| \right\} \cdot \prod_{i=1}^{n'} p_i^{\delta_i}$$

oder

$$\min_x \left\{ |Z(xd') \cap M_{g'}| \right\} = (q-1) \frac{\omega_q(m'/d')}{q+1} + \min_x \left\{ |Z(xd) \cap M_g| \right\} - (q-1) \frac{\omega_q(m/d)}{q+1}$$

$$\geq \min_x \left\{ |Z(xd) \cap M_g| \right\} \cdot \prod_{i=1}^{n'} p_i^{\delta_i}$$

Durch eine leichte Umformung folgt daraus (6).

Corollar 135.1 Die Voraussetzungen wie im vorigen Satz. Es gilt

(i) $\omega_q(m) \cdot D_{\min} \left[\| \|_{q(m'g')} (\overline{g'}) \right] = \omega_q(m') \cdot D_{\min} \left[\| \|_{q(mg)} (\overline{g}) \right]$

(ii) $\omega_q(S) \cdot D_{\min} \left[\| \|_{q(m'g')} (\overline{g'}) \right] = \omega_q(m') \cdot D_{\min} \left[\| \|_{q(Sg)} (\overline{g}) \right]$

mit $S = S(p_1, \ldots, p_n)$ und $k = 0$.

Beweis (i) Ist eine andere Schreibweise für Satz 135 (siehe Lemma 129).
(ii) Folgt aus (i), wenn man $m = S(p_1, \ldots, p_n)$ $(n \geq 1)$ setzt und für $k = 0$ ist dann $m' = S(p_1, \ldots, p_n) \cdot \prod_{i=1}^{n} p_i^{\beta_i}$ $(\beta_i \geq 0)$.

Bemerkung

a. In vielen Beweisen haben wir die p_i bei Bedarf umgeordnet ohne dies jeweils explizit anzugeben.

b. In Satz 131 braucht man sich nicht auf die drei Fälle (i) - (iii) zu beschränken. Es ist vielmehr möglich durch Fallunterscheidung nach den absolut kleinsten Resten den Zusammenhang zwischen $|Z(xd') \cap M_{g'}|$ und $|Z(xd) \cap M_g|$ auszurechnen. Die Berechnungen sind elementar aber langwierig.

c. Durch Satz 135 und Corollar 135.1 hat man die Möglichkeit AN-Codes mit hohem D_{min} und annehmbarer Rate zu finden.

d. Die augmentierten Codes wurden für $q = 2$ von Chien/Hong/Preparata [12] untersucht.

Symboltabelle

$\mathbb{N}$	Natürliche Zahlen (einschließlich 0)
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{R}$	Körper der reellen Zahlen
$\mathbb{Z}_m$	$= \mathbb{Z}/m\cdot\mathbb{Z}$ Restklassenring der ganzen Zahlen modulo m.
$\|M\|$	Mächtigkeit der Menge M (Anzahl der Elemente für endliches M)
(a,b)	Offenes Intervall
$[a,b)$	Halboffenes Intervall
$[a,b]$	Abgeschlossenes Intervall
$d=(n,m)$	Grösster gemeinsamer Teiler (g.g.T.)
$<n, m>$	Kleinstes gemeinschaftliches Vielfaches (k.g.V.)
$n\mid m$	n teilt m
$n\nmid m$	n teilt m nicht
$p^z \parallel m$	$p^z \mid m$ und $p^{z+1} \nmid m$
$a\equiv b \bmod m$	$m \mid (a-b)$ (a, b, m ganze Zahlen)
$\varphi(n)$	Eulersche Funktion (Anzahl aller $x<n$ mit $(x, n) = 1$)
$\mu(n)$	Möbiusfunktion
$\mathfrak{N}(n)$	Anzahl der quadratfreien Teiler von n
$\delta(i,j)$	Kroneckersymbol (= 1 für i = j, = 0 sonst)
$f(x)\sim g(x)$	f(x) ist asymptotisch gleich g(x)
$[\alpha]$	Nächste ganze Zahl unterhalb α (α reell)
R	Kommutativer Ring mit Einselement
R^+	Additive Gruppe des Ringes R
$\mathfrak{a},\mathfrak{m},\mathfrak{p}$	Ideale eines Ringes
(r)	Hauptideal (von $r\in R$ erzeugt)
$\overline{R}$	$= R/\mathfrak{m}$ Restklassenring
$R_1\oplus R_2$	Direkte Summe der Ringe R_1 und R_2
$\overline{r}$	Restklasse mit dem Repräsentanten r ($r\in R$, $\overline{r}\in\overline{R}$)
E	Fehlermenge ($\subset\overline{R}$), p. $\emptyset$
E_c	Menge der zu korrigierenden Fehler; p. $\emptyset$
E_d	Menge der zu entdeckenden Fehler; p. $\emptyset$

g Generator eines AN-Codes im Ring $\mathbb{Z}_{m \cdot g}$ ($m, g > 1$); p. 4

$\| \|$, $\| \|_{ind}$ Norm, k-Pseudobewertung eines Ringes R; p. 10, 12 (ind ist irgendein Index zur genauen Kennzeichnung der speziellen Norm)

$\| \|_{ind\, \mathfrak{a}}$ Modulare Norm auf $R/\mathfrak{a}$, wenn $\| \|_{ind}$ Norm auf R ist; p. 12

$D_{min}[\| \|_{ind\, \mathfrak{a}}\, \mathfrak{v}]$ Minimale arithmetische Distanz; p. 13

$E_c(t)$, $E_d(t)$ p. 14

$B(r,t)$ Sphäre um r mit dem Radius t; p. 14

V_t Volumen von $B(r, t)$ ($= |B(r,t)|$); p. 14

$Rd(m)$ Redundanz eines AN-Codes; p. 15

$Rt(m)$ Rate eines AN-Codes; p. 15

$B(\| \|)$, $S(\| \|)$, $P(\| \|)$ p. 16

NAF Non-Adjacent Form; p. 30

GNAF Generalized Non-Adjacent Form; p. 30

q Basis für die (q-näre) Darstellung der ganzen Zahlen; p.29

$\| \|_q$ q-Norm; p. 30

$M_q(g,d)$ p. 38

$M(g,d)$ $= M_2(g,d)$

$L_q(g)$ p. 38

$L(g)$ $= L_2(q)$

$\omega_q(g)$ Multiplikative Ordnung von q modulo g; p. 38

$\omega(g)$ $= \omega_2(g)$

$D_{min}[0,M)_q$ p. 42

$R(q)$ $= \langle 2,3, \ldots, q-1 \rangle$; p. 48

$R_m(a)$ Kleinster positiver Rest modulo m (a ganze Zahl); p. 50

$\| \|^*_{ind(m)}$ p. 50

$d^*_{ind(m)}$ Metrik; p. 50

CYL_q Zyklischer Linksshift; p. 56

$Z(x)$ Zyklische Klasse von x; p. 58

C Klasse; p. 64

B_j Block der Länge j; p. 67

$N_q(B_j,m)$ Anzahl der Blöcke B_j; p. 67

(j,ε) - normal zur Basis q; p. 74

U(pper)
M(iddle) } Intervalle; p. 76
L(ower)

M_ε Intervall $\left(\frac{m}{q+1},\ q\cdot\frac{m}{q+1}\right]$; p. 83

M_ε/n Intervall $\left(\frac{m}{(q+1)\cdot n},\ q\cdot\frac{m}{(q+1)\cdot n}\right]$; p. 87

$w(m)$ p. 104

$S(p_1,\ldots,p_n)$ Saturations-Produkt; p. 106

$T(n,k)$
$E(k,j,n)$ } Bezeichnungen aus der Theorie der Totative
$y(k,j,n)$ } siehe Holzer [30] pp. 122

Literaturverzeichnis

[1] Avižienis, A. et al.: The STAR (self-testing and repairing) computer: An investigation of the theory and practice of fault-tolerant computer design. IEEE Trans. Computers C-20 (1971) 1312-1321

[2] Avižienis, A.: Arithmetic error codes; Cost and effectiveness studies for application in digital system design. IEEE Trans. Computers C-20 (1971) 1322-1331

[3] Barrows, Jr., J.T.: A new method for constructin multiple error correcting linear residue codes. Report R-277, Coordinated Science Laboratory Univ. of Illinois, Urbana (1966)

[4] Batty, J.S.: Some properties of pure recurring decimals. Math. Gaz. 38 (1954) 90-95

[5] Bialoborski, E.: On circular numbers. (Polish) Wiadom. Mat. (2) 4 (1960) 91-92

[6] Brown, D.T.: Error detecting and error correcting binary codes for arithmetic operations. IRE Trans. Electronic Computers EC-9 (1960) 333 - 337

[7] Brown, Jr., J.L.: Note on complete sequences of integers. Amer. Math. Monthly 68 (1961) 557-560

[8] Brown, Jr., J.L.: Generalized bases for the integers. Amer. Math. Monthly 71 (1964) 973 - 980

[9] Chen, C.L./Chien, R.T./: On the binary representation Liu, C.K. form of certain integers. SIAM J. Appl. Math. 26 (1974) 285 - 293

[10] Chiang, A.C.L./Reed, I.S.: Arithmetic norms and bounds of the arithmetic AN codes. IEEE Trans. Inform. Theory IT-16 (1970) 470 - 476

[11] Chien, R.T.: Linear residue codes for burst error correction.
IEEE Trans. Inform. Theory IT-10 (1964)
127 - 133

[12] Chien, R.T./Hong, S.J./: Some results in the theory of
Preparata, F.P. arithmetic codes
Information And Control 19 (1971)
246 - 264

[13] Chin-Long Chen: An asymptotic bound on the distance of arithmetic codes.
IEEE Trans. Inform. Theory IT-20 (1974)
253 - 254

[14] Clark, W.E./Liang, J.J.: On arithmetic weight for a general radix representation of integers.
IEEE Trans. Inform. Theory IT-19 (1973)
823 - 826

[15] Clark, W.E./Liang, J.J.: On modular weight and cyclic nonadjacent forms for arithmetic codes.
IEEE Trans. Inform. Theory IT-20 (1974)
767 - 770

[16] Cohn, P./Mahler, K.: On the composition of pseudo-valuations.
Nieuw Arch. v. Wiskunde (3) 1 (1953)
161 - 198

[17] Dadaev, Yu.G.: On the theory of cyclic arithmetical codes.
Problems of Information Transmissions 6
(1970) 37 - 42 (1972)

[18] de Bruijn, N.G.: On bases for the set of integers.
Publ. Math. (Debrecen) 1 (1950) 232 - 242

[19] Diamond, J.L.: Checking codes for digital computers.
Proc. IRE 43 (1955) 487 - 488

[20] Dynkin, V.N./Kimelfeld, B.N.: Construction of nonbinary arithmetic codes that correct individual errors. (Russian)
Problemy Peredači Informacii 9 (1973)
vyp. 1, 22 - 25

[21] Garcia, O.N.: Error codes for arithmetic and logical operations.
Ph. D. Thesis, Report D-69-03, Univ. of Maryland, College Park (1969).

[22] Garner, H.L.: Error codes for arithmetic operations.
IEEE Trans. Electronic Computers EC-15 (1966) 763 - 770

[23] Goto, M./Fukumura, T.: The distance of arithmetic codes.
Memoirs Faculty of Engineering, Nagoya Univ. (Japan) 20 (2) (1968) 474 - 482

[24] Goto, M./Fukumura, T.: Nonbinary AN codes with distance not less than five.
IEEE Trans. Inform. Theory IT-19 (1973) 129 - 134

[25] Goto, M./Fukumura, T.: Perfect nonbinary AN codes with distance three.
Information And Control 27 (1975) 336-348

[26] Gritsenko, V.M.: Nonbinary arithmetic correcting codes.
Problems of Information Transmissions 5 (1969) 15 - 22

[27] Hartman, W.F.: Modular arithmetic weight and cyclic shifting.
Information And Control 21 (1972) 339-343

[28] Hartmann, C.R.P./: A bound for arithmetic codes of
Tzeng, K.K. composite length.
IEEE Trans. Inform. Theory IT - 18 (1972) 308

[29] Hoggatt, Jr., V.E.: Generalized Zeckendorf theorem.
Fibonacci Quart. 10 (1972) no. 1, 89 - 93

[30] Holzer, L.: Zahlentheorie III. (§ 14 - 15)
B.G. Teubner Verlagsgesellschaft, Leipzig (1965)

[31] Huckaba, J.A.: Extensions of pseudo-valuations.
Pacific J. Math. 29 (1969) 295 - 302

[32] Keller, T.J.: Generalizations of Zeckendorf's theorem. Fibonacci Quart. 10 (1972) no. 1, 95 - 102, 111, 112

[33] Kondratyev, V.N./: Error-correcting codes with a Peterson
Trofimov, N.N. distance not less than five.
Eng. Cybernetics 3 (1969) 85 - 91

[34] La Barbera, Sal: Fibonacci, Lucas and the Egyptians. Fibonacci Quart. 9, 2 (1971) 177-187, 194

[35] Leavitt, W.G.: A theorem on repeating decimals. Amer. Math. Monthly 74 (1967) 669 - 673

[36] Le Veque, W.J.: Topics in Number Theory. Vol. I. Addison-Wesley, Reading, Mass. (1956)

[37] Long, C.T./Woo, N.: On bases for the set of integers. Duke Math. J. 38 (1971) 583 - 590

[38] Mahler, K.: Über Pseudobewertungen, I. Acta math. 66 (1936) 79 - 199

[39] Mahler, K.: Über Pseudobewertungen, Ia. Akad. Wetensch. Amsterdam, Proc. 39 (1936) 57 - 65

[40] Mahler, K.: Über Pseudobewertungen, II. Acta math. 67 (1936) 51 - 80

[41] Mahler, K.: Introduction to p-adic numbers and their functions. Cambridge University Press (1973)

[42] Mandelbaum, D.: Arithmetic codes with large distance. IEEE Trans. Inform. Theory IT-13 (1967) 237 - 242

[43] Massey, J.L.: Survey of residue coding for arithmetic [illegible] Computation Center Bulletin 3 (IBM SEO, Rome, Italy) (1964) 3-17

[44] Massey, J.L./Garcia, O.N.: Error correcting codes in computer arithmetic.
Advances in Information Systems Science (Ed. J. Tou), New York: Plenum Press (1972) Chap. 5, pp. 273 - 326

[45] Müller, H.: Zur gleichmässigen Verteilung der Totative. I, II.
Wiss. Z. Pädagog. Hochschule Potsdam Math.-Natur. Reihe 8 (1963/64) 71-76, 77-81

[46] Nelson, R.: Pseudovaluations of Polynomials.
Canad. J. Math. 19 (1967) 1293 - 1302

[47] Neumann, P.G./Rao, T.R.N.: Error correcting codes for byte-organized processors.
IEEE Trans. Computers C-24 (1975) 226-232

[48] Peinado, R.E.: On finite rings.
Math. Mag. 40 (1967) 83 - 85

[49] Peterson, W.W.: Error-correcting codes.
M.I.T. Press and Wiley, Cambridge, Mass. New York (1961)

[50] Plotkin, B.I.: Groups of automorphisms of algebraic systems. Chap. 2
Wolters-Noordhoff Publ., Groningen (1972)

[51] Preparata, F.P.: On the representation of integers in nonadjacent form.
Information and Control 19 (1971) 246-264

[52] Rao, T.R.N./Trehan, A.K.: Single - error - correcting nonbinary arithmetic codes.
IEEE Trans. Inform. Theory IT-16 (1970) 604 - 608

[53] Rao, T.R.N./Garcia, O.N.: Cyclic and multiresidue codes for arithmetic operations.
IEEE Trans. Inform. Theory IT-17 (1971) 85 - 91

[54] Rao, T.R.N.: Error coding for arithmetic processors. Academic Press, New York and London (1974)

[55] Rees, D.: Valuations associated with a local ring (I). Proc. London math. Soc. (3) 5 (1955) 107-128

[56] Rees, D.: Valuations associated with a local ring (II) J. London math. Soc. 31 (1956) 228 - 235

[57] Rees, D.: Valuations associated with ideals (II). J. London math. Soc. 31 (1956) 221 - 227

[58] Reitwiesner, G.H.: Binary arithmetic. Advances in Computers Vol. 1 (Ed. F.L.Alt) New York: Academic Press (1960) pp. 232-308

[59] Riesel, H.: Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$. Math. Comp. 18 (1964) 149 - 150

[60] Sangare, D.: Théorie des valuations. C.R. Acad. Sc. Paris 276 (1973) A981-A984

[61] Seguin, G.: Bounds for certain cyclic AN-codes. Information And Control 23 (1973) 41-47

[62] Stoneham, R.G.: The reciprocals of integral powers of primes and normal numbers. Proc. Amer. Math. Soc, 15 (1964) 200-208

[63] Stoneham, R.G.: On (j, ξ) - normality in the rational fractions. Acta Arithmetica 16 (1970) 221 - 237

[64] Szipro, L.: Fonctions d'ordre et valuations. Bull. Soc. math. Fr. 94 (1966) 301-311

[65] Tenengolts, G.M./: Cyclic codes which correct arithmetic Dynkin, V.N. errors. Problems of Information Transmissions 6 (1970) 219 - 222 (1973)

[66] Tsao-Wu, N.T.: Arithmetic cyclic codes.
Ph. D. Thesis, Department of Electrical Engineering, Northeastern Univ., Boston, Mass. (June 1968)

[67] Vandiver, H.S./: Introduction to arithmetical factori-
Weaver, M.W. zation and congruences from the standpoint of abstract algebra.
Amer. Math. Monthly 65 (1958) no. 8, part II, 53 pp.

[68] Wolf, J.K.: A survey of coding theory: 1967-1972.
IEEE Trans. Inform. Theory IT-19 (1973) 381 - 389

[69] Zeckendorf, E.: A generalized Fibonacci numeration.
Fibonacci Quart. 10 (1972) no. 4, 365-372

Lebenslauf

31.12.1937	Geboren in Gumbinnen / Ostpr.
Vater:	Paul Ecker, Verwaltungsangestellter
Mutter:	Hilde Ecker, geb. Michel

Schulbesuch:

1943-1944	Grundschule in Gumbinnen
1945-1950	Grundschule in Grimmen / Vorpommern
1950-1957	Droste-Hülshoff-Gymnasium / Berlin-Zehlendorf
20.2.1957	Abitur

Studium:

Studienfächer:	Mathematik und Physik
SS 1957 - WS 1963/64	FU - Berlin

Abgelegte Prüfungen:

29.10.1964	1. Staatsexamen (Hauptfach Mathematik)
9. 2.1967	Diplom in Mathematik

Weitere Tätigkeit:

1965-1967	Studienreferendar
1967-1969	Wiss. Angestellter am Rechenzentrum der DFVLR / Forschungszentrum Braunschweig
1969-	Wiss. Angestellter im Sektor Mathematik des HMI - Berlin